MPR 1600.1
REVISION C
EFFECTIVE DATE: September 27, 2004
EXPIRATION DATE: September 27, 2009

MARSHALL PROCEDURAL REQUIREMENTS

AD01

MSFC SECURITY PROCEDURAL REQUIREMENTS

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Baseline		8/16/99	
Revision	A	4/28/00	This revision changes "Applicable Documents" "a." from NHB 1620.3 to NPG 1620.1. Under "Definitions" a definition for Administratively Controlled Information (ACI) has been added and the Definition for "FOR OFFICIAL USE ONLY" has been changed. In Chapter 1, paragraph 1.18 has been added to cover ACI. In Chapter 10, paragraph 10.2.3.4, "Privacy Act Information" has been deleted and "Administratively Controlled Information" has been substituted. In Chapter 12, paragraph 12.3.3.3.b has been changed to increase insurance amount for Michoud. In Chapter 13, paragraph 13.3.5.3 has been reworded.
Revision	B	4/2/2004	Document totally revised to incorporate changes mandated by HQ and to reflect current procedures.
Revision	C	9/27/2004	To change procedures to requirements, adhere to Directives Review Standards, change some points in traffic points table, change Lock and Key requests to the Service Request System, and remove ambiguity.

TABLE OF CONTENTS

PREFACE

P.1 PURPOSE

To assist employees in finding answers to basic security questions, learn personal responsibilities for security, and provide uniform procedures and guidance to assist every employee in the implementation of an effective Marshall Space Flight Center (MSFC) security program.

P.2 APPLICABILITY

This document is applicable to all MSFC organizational elements, associated contractors, other assigned Government employees, contractor sites under MSFC operational jurisdiction, and visitors to MSFC.

P.3 AUTHORITY

42 U.S.C. 2455, 2456, 2456A, and 2473(c), Section 304 and 203(c), respectively, of the National Aeronautics and Space Act of 1958, as amended.

P.4 APPLICABLE DOCUMENTS

a. NPR 1620.1, “Security Procedural Requirements”

b. NPR 1441.1, “NASA Records Retention Schedules”

c. MPR 2810.1, “Security of Information Technology”

d. MPR 1371.1, “Procedural Requirements for Processing Foreign Visitor Requests”

e. NPD 1660.1, “NASA Counterintelligence (CI) Policy”

P.5 REFERENCES

a. DOD 5220.22M, “National Industrial Security Program Operating Manual (NISPOM)”

b. AMCOM Regulation 210-1, “Post Regulations””

P.6 CANCELLATION

MPG 1600.1B, dated April 2, 2004

Original signed by
Robin N. Henderson for

David A. King
Director

DOCUMENT CONTENT

1. DEFINITIONS

1.1 Access. Access is a person's ability and opportunity to gain knowledge of classified information or enter a controlled access area.

1.2 Access Control. The means, through a variety of procedures and equipment, to regulate and monitor the movement of personnel and/or vehicle traffic through points of entry and exit.

1.3 Accountable Records Custodian (ARC). The person responsible for ensuring the accountability and control of all accountable classified material within MSFC. The ARC manages the MSFC Classified Document Control and serves as the centralized location for processing classified documents.

1.4 Administratively Controlled Information (ACI). Official information and material, of a sensitive but unclassified nature, which does not contain national security information (and therefore cannot be classified), nonetheless, should still be protected against inappropriate disclosure. (See paragraph CH1.18.4 for criteria for ACI designations).

1.5 Adverse Information. Any information that reflects adversely on the integrity or character of the employee, which suggests that his or her ability to safeguard classified information may be impaired.

1.6 Area Manager. The Director/Manager of organization who controls access to a controlled access area as designated by the Protective Services.

1.7 Assigned Government or Company Vehicle Space. A parking space reserved for government or company vehicles assigned to organizations or companies served by the parking lot. The spaces are clearly marked ASSN GOV VEHICLE or ASSN CO VEHICLE.

1.8 Authorized Person. A person who is appropriately cleared, has a valid need-to-know, and has been granted access to an area by appropriate persons.

1.9 Authorized Parking Space. A parking space identified by a bumper block, by markings on a curb, lines painted on the pavement, or other specially designated parking areas. Parking is prohibited in any area not so marked, or on grassy areas.

1.10 Background Investigation. The means or procedures, such as selective investigations, record checks, personal interviews, designed to provide reasonable assurance that persons being considered for or granted access to classified information are loyal and trustworthy.

1.11 Classified Information. Classified information is any information or material, regardless of its physical form or characteristics, that is owned, produced, or is under the control of the United

States Government, and is determined to require protection against unauthorized disclosure in the interests of national security, and is so designated.

1.12 Classified Working Document. A classified working document is any product, regardless of its physical form or characteristics, that is accumulated or created during the preparation of a finished classified document. Examples of classified working documents are notes, drafts, and rough drawings, and may be in the form of disks, tapes, films, and other similar media.

1.13 Closed Area. An area in which security measures are taken to safeguard classified material where entry to the area alone provides visible or audible access to classified information.

1.14 Cognizant Security Office. The office having primary responsibility for exercising control over industrial security matters at a contractor facility.

1.15 Communications Security (COMSEC). The application of security measures to deny an unauthorized person any information of value which might be derived from the possession of and study of telecommunications, or to ensure the availability and authenticity of telecommunications.

1.16 Compromise. A breach of security due to an unauthorized person gaining knowledge of classified information.

1.17 Component Facility. A NASA owned or leased facility that is not contiguous to a NASA Center, and is in operation to support NASA missions (e.g., remote sensing sites, conference and/or other meeting, mission, or support activities, etc.).

1.18 COMSEC Compromise. A very serious breach of security due to an unauthorized individual gaining knowledge of classified information. Security can be compromised by the misuse or improper handling of COMSEC material, or any act or omission in conflict with established COMSEC policies and procedures.

1.19 Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, and international or domestic terrorist activities.

1.20 Counterterrorism. Information gathered and activities conducted to protect against terrorist threats and incidents conducted by domestic or international groups or individuals.

1.21 Custodian. Any authorized person who possesses and is charged with responsibility for safeguarding or accounting for classified information or material.

1.22 Derivative Classification. The determination that information is the same as information currently classified, and therefore requires the application of classification markings. This term

includes the act of incorporating, paraphrasing, restating, or generating this information in a new format.

1.23 Designated Areas. Certain countries with policies that have been determined to be inimical to U.S. interests. NASA Headquarters will periodically inform Protective Services of this list of countries and will, as necessary, advise them of any changes that occur.

1.24 Espionage. The act of obtaining, delivering, transmitting, communicating, or receiving information in respect to national defense with the intent or reason to believe that the information may be used to the injury of the United States or the advantage of any foreign nation. The offense of espionage applies in times of war or peace.

1.25 Facility Security Clearance. An administrative determination that an industrial facility is eligible for access to classified information up to and including a designated category.

1.26 Foreign National. Any person who is not a citizen of the United States.

1.27 Foreign Representative. Any person, including a U.S. citizen or permanent resident alien of the United States, who seeks to visit NASA Centers for the purpose of representing a government, business, organization, or person of a country other than the United States. It should be noted that a permanent resident alien is a foreign national who has been issued a "Green Card" or work permit for permanent work in the U.S. but is not a U.S. citizen.

1.28 For Official Use Only. A notation used on information and material, from agencies and departments outside NASA, which requires protection against disclosure to unauthorized persons or release to the public.

1.29 Handicapped Parking Space. A parking space for individuals with a state-issued tag/placard or MSFC-issued temporary handicapped permit issued by the MSFC Equal Opportunity Office (EEO).

1.30 Industrial Security. The application of Government security practices, procedures, and requirements within the industrial, outsourced, or contractor arena.

1.31 Information Technology Security (ITS). Encompasses all security features needed to provide an acceptable level of protection for hardware, software, and information used for the processing of sensitive and classified data in an automated information system. It includes all hardware and software functions, characteristics, and features; operational procedures, accountability procedures, and access controls at all ITS facilities, including those housing mainframes, terminals, minicomputers, or microcomputers. Management constraints include physical protection, control of harmful emissions, personnel security, and communications security.

1.32 Inside Fenced/Barricade/Barrier Areas. No privately owned vehicles (POV) are authorized to park inside fenced areas except those belonging to handicapped employees, service vehicles, and a limited number of reserved, visitors, and transient parking spaces.

1.33 Limited Area. An area in which security measures are taken to safeguard classified material or unclassified property warranting special protection. To prevent unauthorized access to such property, visitors may be escorted or other internal restrictions implemented, as determined by the Manager, Protective Services.

1.34 Marshall Access Control System (MACS). A microprocessor-based system of electromechanical and electronic devices that monitor and permit or deny access to a controlled access area by personnel or vehicles following the introduction of a coded identification badge to a mounted card reader.

1.35 Mission Essential Infrastructure (MEI). Critical resources/assets that the Agency depends on to perform and maintain its most critical missions. These resources may include critical components and facilities associated with the Space Shuttle, expendable launch vehicles, associated upper stages, Spacelab, International Space Station, command communication and control capability, Government-owned flight or experimental flight vehicles and apparatus, and one-of-a-kind irreplaceable facilities.

1.36 Mission Essential Infrastructure Protection Program (MEIPP). The planning and implementation of an enhanced protection level for Agency MEI identified as being so crucial to the success of NASA missions as to warrant protection over that which is routinely provided to domestic and foreign NASA facilities.

1.37 National Security. The national defense or foreign relations of the United States.

1.38 Need-to-Know. A determination made by the possessor of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of classified information in order to perform tasks or services essential to the fulfillment of a classified contract or program approved by NASA/MSFC.

1.39 Original Classification. The initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure, including a classification designation signifying the level of protection required.

1.40 Parking Space. Space identified by bumper blocks, markings on a curb, or lines painted on the pavement. Parking is prohibited in any area not so marked or on grassed areas.

1.41 Personnel Security Investigation. Any investigation required for determining the eligibility of MSFC personnel and contractor employees to have access to classified or sensitive information, to be assigned to or retained in sensitive duties, or to perform other designated duties requiring an investigation. A personnel security investigation may also include an

investigation into an allegation arising subsequent to an adjudicative action which requires resolution in order to determine an individual's current eligibility for access to classified information or for assignment to, or retention in, a sensitive position.

1.42 Physical Security. All security measures, of a physical nature, implemented to protect critical assets. Specific measures may include actions such as controlled access via security officers or magnetic card access systems, security escorts for shipment of sensitive items, surveillance cameras, or other appropriate measures.

1.43 Probable Compromise. Exists when a compromise of classified information cannot be firmly established, but a reasonable presumption exists that an unauthorized person has had access to classified information.

1.44 Regrade. To assign a higher or lower security classification to an item of classified material.

1.45 Report of Incident (ROI). A report written by Protective Services for any infraction of security guidelines and procedures, accidents, incidents, violations, etc.

1.46 Restricted Area. An area in which security measures are taken to safeguard and control access to property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. All facilities designated under the MEI Protection Program shall be "Restricted" areas (as a minimum designation).

1.47 Sabotage. The act of injuring, destroying, contaminating, or infecting any national defense material, premises, or utilities with the intent to injure, interfere with, or obstruct the national defense of the United States; or, making, constructing, or causing to be made or constructed in a defective manner any national defense material, premises, or utilities with the intent to injure, interfere with, or obstruct the national defense of the United States. The offense of sabotage applies in times of war or peace.

1.48 Security Area. A physically defined area, established for the protection of facilities, property, or classified information and material in the possession or custody of NASA, MSFC, or a NASA contractor located at a NASA installation or component installation, entry to which is subject to security measures, procedures, or controls.

1.49 Security Classification Guide (SCG). A document issued by an authorized original classifier. The Guide will prescribe the level of classification and appropriate declassification instructions for specified information to be classified on a derivative basis.

1.50 Security Hazards. Conditions that permit the unauthorized access to a sensitive or closed area by uncleared or unauthorized personnel, giving them the opportunity to install a surveillance device, exploit existing equipment, or conduct covert operations.

1.51 Security Violation. A failure to comply with or observe policies and procedures specifically established for safeguarding classified information, but which has not resulted in a compromise or probable compromise of classified information.

1.52 Security Survey. A comprehensive formal evaluation of a facility, area, or activity by security specialists to determine its physical or technical strengths and weaknesses and to propose recommendations for improvement.

1.53 Sensitive Areas. Areas where physical security measures have been employed to preclude the unauthorized access to proprietary/sensitive material (e.g., procurement offices, investigator general offices, or source evaluation board areas, ACI).

1.54 Sensitive Information/Material. Unclassified information or material determined to have special protection requirements to preclude unauthorized disclosure to avoid compromises, risks to facilities, projects or programs, threat to the security and/or safety of the source of information, or to meet access restrictions established by laws, directives, or regulations.

1.55 Service Vehicle Parking Space. A parking space reserved for government service vehicles, other government vehicles, vehicles of companies doing business with MSFC which have the company name marked thereon, and vehicles having MSFC Service Vehicle Permits issued by MSFC Protective Services. Parking is **LIMITED TO TWO HOURS** unless otherwise posted.

1.56 Transient Parking Space. A parking space reserved for vehicles operated by persons who are not assigned to the building, area, or complex, which the parking lot serves. Parking is **LIMITED TO TWO HOURS** unless otherwise posted. For example, if you are assigned to any building in the 4200 complex, you are authorized to park in transient at other buildings, but not at the 4200 complex.

1.57 Technical Surveillance Countermeasure (TSCM) Program. Includes measures taken to prevent, detect and locate attempted or actual technical surveillance penetrations. A TSCM survey may include a thorough physical, electronic, and visual examination.

1.58 Terrorism. The unlawful use or threatened use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. Terrorism may be categorized as domestic or international depending on the origin, base, and objectives of the terrorists.

1.59 Unauthorized Person. Any person not authorized to have access to specific classified information or to a designated controlled access area.

1.60 Visitor Parking Space. A parking space reserved for non-decaled vehicles operated by a person who does not have, and is not authorized, an MSFC or Redstone Arsenal vehicle decal.

Visitors that are issued a one-day Temporary Vehicle Pass at Redstone gates or a long-term pass by Protective Services are authorized to park in these marked areas.

1.61 Waiver. The approval of the Risk Acceptance Authority to continue a condition that varies from a requirement and creates vulnerability.

2. RESPONSIBILITIES

2.1 Protective Services shall administer policies and procedures, and conduct investigations as necessary for the protection of personnel, information, and property of MSFC. It shall control visitors and access, adjudicate security clearances, provide security education, administer the Personnel Reliability Program clearances, issue identification badges and decals, and enforce traffic regulations. Protective Services shall also administer the Mission Essential Infrastructure Protection Program (MEIPP), control international visits, interface with federal and local law enforcement agencies, and conduct counterintelligence investigations, as necessary. The Manager, Protective Services shall serve as the TSCM Program authority, ensure Federal Arrest Authority (FAA) is properly administered, and act as the Center Certifying Official for the authority to carry and use concealed or unconcealed firearms by security forces, both NASA civil service personnel and contractor.

2.2 Employees shall:

Become familiar with and follow the procedures outlined in this MPR and in NPR 1620.1.

2.3 Managers/Supervisors shall:

2.3.1 Ensure attendance of their employees at scheduled security briefings or training.

2.3.2 Periodically review pertinent security regulations with employees, pointing out new or revised requirements.

2.3.3 Immediately report any knowledge of a compromise or a failure to comply with any of the policies, procedures, or requirements in this procedure.

2.3.4 Ensure that employees under their supervision who transfer, terminate employment, take extended leave, or retire from MSFC are processed through Protective Services and receive the required debriefings.

2.3.5 Consult with Protective Services on any action to safeguard classified information or critical hardware/software.

2.3.6 Notify Protective Services of any special security provisions that may be required for upcoming projects, programs, or studies.

2.3.7 Request assistance from Protective Services when devising internal security procedures required by their organization.

2.3.8 Notify Protective Services of adverse information concerning employees having access to classified information, or information that may impact the safety of other employees.

3. PROCEDURE

See Chapters 1 through 17.

4. RECORDS

4.1 Personnel Security Investigation Files and related forms and correspondence shall be retained in Protective Services in accordance with NPR 1441.1, NRRS 1/103(A).

4.2 Classified Document Accountability Records and related files shall be retained in Protective Services in accordance with NPR 1441.l, NRRS 1/111(B).

4.3 Badging and Decal Records shall be maintained by the Protective Services' support contractor until the employee clears the center, then the records are held for 6 months and destroyed.

4.4 Visitor records shall be retained by the Protective Services' support contractor in accordance with NPR 1441.1, NRRS 1/114 (A.2).

4.5 Traffic Violation Records shall be retained by the Protective Services' support contractor for 2 years and then destroyed.

4.6 Reports of Incident shall be retained by Protective Services in accordance with NPR 1441.1, NRRS 1/107.

4.7 Copies of DD Forms 254, "DOD Contract Security Classification Specification," shall be retained in Protective Services Office in accordance with NPR 1441.1, NRRS 1/113(B).

4.8 Lock and Key Database and related correspondence shall be retained by the Protective Services' support contractor and Protective Services in accordance with NPR 1441.1, 1/99(B).

4.9 Firearms accountability records shall be maintained in Protective Services in accordance with NPR 1441.1, NRRS 1/106(B).

4.10 Badging Signature Authorizations shall be maintained by the Protective Services' support contractor on a current basis and destroyed when no longer needed.

5. FLOW DIAGRAM

None

Chapter 1

SAFEGUARDING CLASSIFIED AND ACI INFORMATION

CH1.1 General

MSFC shall provide protection for sensitive and accountable classified documents/material/information, working documents, or by-products commensurate with the assigned classification level; prevent unauthorized persons from gaining access during its use, dissemination, storage, movement, or transmission. Only those persons who have been granted the appropriate level of security clearance and have a need-to-know shall be granted access to classified information.

CH1.2 Responsibilities

CH1.2.1 Protective Services shall:

CH1.2.1.1 Provide functional oversight of the Information Security Program to ensure classified national security information is afforded adequate protection to prevent compromise, and that sensitive information is safeguarded.

CH1.2.1.2 Appoint a Classified Material Control Officer (CMCO) and alternate and establish and administer the MSFC Security Control Point (SCP) for classified material control and accountability.

CH1.2.1.3 Ensure an inventory of accountable material is conducted during annual Information Security Surveys of functional document control stations.

CH1.2.1.4 Conduct preliminary inquiries and formal investigations, as required, when a compromise or suspected loss of classified information occurs.

CH1.2.2 The Classified Material Control Officer (CMCO) shall:

CH1.2.2.1 Function as the central administrative organization records repository for controlling all accountable classified material. CMCO shall enter all accountable incoming classified information into the automated security information management system and transfer outgoing accountable material to outside agencies.

CH1.2.2.2 Provide training and guidance to appointed document custodians on their responsibilities for handling and safeguarding classified information.

CH1.2.2.3 Conduct periodic Information Security surveys and inspections.

CH1.2.2.4 Notify the Manager, Protective Services, immediately upon discovering that a classified document is unaccounted for, or of other security concerns.

CH1.2.3 Supervisors of Custodians shall:

CH1.2.3.1 Establish a Document Control Station (DCS) and appoint a Document Control Station Officer (DCSO) and alternates, as necessary to control classified material within their area.

CH1.2.3.2 Ensure custodians conduct an annual inventory of accountable material and notify Protective Services of the results.

CH1.2.3.3 Ensure that employees under their jurisdiction to whom classified information is entrusted are fully knowledgeable of, and comply with, the provision of this procedure.

CH1.2.4 The DCSO shall:

CH1.2.4.1 Function as the chief interface with Protective Services CMCO on matters pertaining to classified material.

CH1.2.4.2 Understand and comply with the requirements for safeguarding and handling classified information.

CH1.2.4.3 Be designated in writing by each MSFC organization processing or maintaining classified material.

CH1.2.4.4 Possess a security clearance at least equal to the level of the classified material being processed or stored.

CH1.2.4.5 Attend DCSO training conducted by Protective Services within 30 days of appointment and during scheduled refresher training.

CH1.2.4.6 Conduct a joint inventory of classified holdings when a new DCSO is appointed.

CH1.2.4.7 Immediately report any loss or suspected compromise of classified information to Protective Services.

CH1.3 Accountability and Control

CH1.3.1 Protective Services shall establish procedures to ensure accountability of classified documents, prevent unauthorized access to classified information, and provide an audit trail. Protective Services shall serve as central control for maintaining records and controlling classified material received by, and dispatched from, MSFC.

CH1.3.2 The accountability system shall include DCS, as necessary, to place permanent custody of SECRET or CONFIDENTIAL documents as close to the DCSO as possible.

CH1.3.3 With the concurrence of Protective Services, DCSOs may elect to have assigned classified documents maintained by Protective Services. Custodians shall certify need-to-know access by other MSFC employees prior to release of classified documents.

CH1.4 Accountable Classified Material

CH1.4.1 TOP SECRET or SECRET information/documents shall be subject to formal accountability when received from an outside agency, generated internally, or reproduced.

CH1.4.2 SECRET working documents are subject to formal accountability when released outside the directorate or comparable office level, when retained for more than 180 days from creation, or when permanently filed.

CH1.4.3 TOP SECRET working documents shall be subject to the same accounting, control and marking requirements prescribed for a finished document.

CH1.5 Accountability of TOP SECRET Material

CH1.5.1 The Manager, Protective Services is designated as the TOP SECRET Control Officer (TSCO). The TSCO shall ensure that all Center TOP SECRET material/information is accounted for, protected, and transmitted under a chain of receipts, using NASA Form 387, "Classified Material Receipt," covering each individual who is to assume custody.

CH1.5.2 TOP SECRET material may be temporarily loaned on a daily basis to appropriately cleared persons with a valid need-to-know. The material shall be returned to the TSCO at the end of each workday.

CH1.5.3 TOP SECRET documents shall be either under the personal control of a cleared person or stored in an approved container at all times.

CH1.5.4 The TSCO shall conduct a semi-annual inventory of TOP SECRET material, and upon designation of a new TSCO.

CH1.5.5 Sensitive Compartmentalized Information (SCI) shall also be managed by Protective Services. Specific SCI programs at the Center shall operate under specific guidelines tailored for that program.

CH1.6 Accountability of SECRET Material

CH1.6.1 Transfer of accountability of SECRET documents shall be conducted and recorded by Classified Document Control. Transfer of accountability refers to the movement of permanent

custody of a classified document from one DCSO to another, or from a DCSO to an outside agency. The DCSO shall deliver the document to Protective Services for transfer.

CH1.6.2 A unique accountability control number shall be assigned to the classified material, which shall remain in effect as long as the material remains under the MSFC accountability system, regardless of its on-site location.

CH1.6.3 Revisions, supplements, and other material created and added to an existing accountable document shall be assigned the same accountability control number as the original material.

CH1.6.4 Superseding material, which replaces the original classified material, shall be assigned a new accountability control number.

CH1.7 Accountability of CONFIDENTIAL Material

CH1.7.1 CONFIDENTIAL information shall be entered into formal accountability and controlled accordingly if it arrives from an outside agency as an accountable document, or if special category caveats, e.g., RESTRICTED DATA, are included. Use of a receipt during transmission of CONFIDENTIAL other than outlined above is at the discretion of the custodian.

CH1.8 Dissemination of Classified Accountable Material

CH1.8.1 Employees shall disseminate information to other employees and to associated contractors, excluding foreign nationals, who possess a security clearance equal to or higher than the classification of the information to be disseminated, have a valid need-to-know, and have approved storage capability. A need-to-know is a requirement for access to classified information on the basis that it is essential in the performance of an individual's official duty assignment. Supervision in and of itself does not satisfy the need-to-know requirement.

CH1.8.2 The responsibility for determining whether an individual's official duties require possession of, or access to, any element or item of classified information shall rest upon the individual who has authorized possession, knowledge, or control of the information.

CH1.8.3 Classified material originated by an agency outside NASA shall not be disseminated to another agency without the consent of the originating agency, unless permitted by Memorandum of Agreement between the parties involved, or an instruction included with the document.

CH1.9 Dissemination of Information at Classified Meetings

CH1.9.1 Prior to discussing classified information, the person responsible for the meeting shall ensure:

- Protective Services has approved a Classified Meeting Room

- All attendees are cleared to the appropriate level
- All attendees have a need-to-know
- Doors are closed as necessary to deny access to passersby
- The classification of the meeting is announced
- All visual aids are marked with appropriate classification
- All classified handouts are properly marked
- There are no electronic transmitting or any other recording devices in the room

CH1.9.2 During the meeting the person responsible for the meeting shall:

- Deny entry and access to unauthorized individuals
- Ensure that security is maintained during breaks
- Ensure no electronic transmitting devices or other recording devices are allowed

CH1.9.3 After the meeting the person responsible for the meeting shall:

- Remind all attendees of the security classification level
- Advise all attendees of the prohibition against hand-carrying classified material unless cleared by Protective Services
- Inspect the room thoroughly to ensure that classified material has not been left behind

CH1.10 Temporary Loan (Charge-Out) of Classified Material

Charge-out refers to the temporary loan of an accountable document to an authorized user by the DCSO responsible for accountability of the document. The following procedures shall apply:

CH1.10.1 SECRET and CONFIDENTIAL material may be temporarily charged out to an authorized individual with approved storage capability for a maximum of five workdays. TOP SECRET material may be charged out on a daily basis, only as necessary for review, coordination, or similar action.

CH1.10.2 The material shall be hand-delivered or picked up by an employee possessing the appropriate level security clearance, need-to-know, and approved storage container, or delivered to Classified Document Control for further accountability and distribution.

CH1.10.3 The recipient shall be responsible for safeguarding the classified material until it is returned to the DCSO. Users not having approved storage capability shall return the loaned document to the DCSO before the end of each workday.

CH1.11 Transmittal of Classified Accountable Material

CH1.11.1 Transmittal to Outside Facilities

CH1.11.1.1 SECRET and CONFIDENTIAL material shall be delivered to Protective Services Classified Document Control and transmitted by approved methods to authorized persons or agencies outside of MSFC.

CH1.11.1.2 Bulky classified material and hardware shall be wrapped, boxed, or crated to prevent exposure of the material.

CH1.11.2 Transmission by Secure Facsimile or Secure Network

SECRET or CONFIDENTIAL material may be transmitted on an approved secure facsimile or secure network. Contact Protective Services for the location of an approved facsimile station.

CH1.11.3 Transmission by Commercial Carriers

Protective Services shall approve all shipments of classified material via an approved commercial carrier. The request shall be made as far in advance as possible to allow sufficient time for accountability, material processing, and coordination with transportation for additional protection measures, as required.

CH1.11.4 Transmission by Designated Couriers

The transmittal of classified material outside MSFC by appropriately cleared couriers shall be coordinated and approved by Protective Services in advance of the scheduled trip. The following procedures shall apply for hand-carrying of classified material by MSFC employees on official travel status:

CH1.11.4.1 The hand-carrying of classified material shall be approved on a case-by-case basis. Classified material may be hand-carried aboard a U.S. Government-owned or chartered aircraft on a domestic or international flight with the approval of the Manager, Protective Services.

CH1.11.4.2 When time does not permit the mailing of classified material, the document may be hand-carried. The request shall be submitted to Protective Services, along with the material to be hand-carried, for approval and other required actions.

CH1.11.4.3 Employees authorized to sign for and hand-carry classified material, shall be given a courier briefing by Protective Services on their responsibilities to safeguard the classified material. After being briefed, the courier shall be given a letter of authorization.

CH1.11.4.4 The original courier authorization letter shall be retained by the courier at all times while hand-carrying the material. A copy shall be retained by Protective Services, and the third copy shall be retained by the requesting official. The courier shall comply with all security requirements necessary to protect the material.

CH1.11.4.5 The material shall be packaged in the same manner as classified material being transmitted through the mail. When the package is opened during the course of a trip and the contents are to be hand-carried back to MSFC, the courier shall ensure the material is appropriately marked and repackaged prior to departure.

CH1.11.4.6 When the accountable material is to be retained by an outside agency, Protective Services shall prepare a classified material receipt in advance. The courier shall obtain a signature by the recipient and return the signed receipt to Protective Services upon return to MSFC.

CH1.11.4.7 If the courier shall remain overnight, Protective Services shall assist in arrangements for approved storage of the classified material.

CH1.12 Storage of Classified Accountable Material

CH1.12.1 Classified information shall be under the immediate control and observation of an authorized person, or stored in an approved container or controlled access area designed to preclude unauthorized access. Classified information shall never be left unattended outside an approved container.

CH1.12.2 Containers approved for storage of classified material, to include classified waste, shall be General Services Administration (GSA) approved with three-position combination lock.

CH1.12.2.1 When it is impractical to store classified material as defined, Protective Services shall prescribe special storage requirements due to the size, bulk, or nature of the classified material. Supplemental controls, as required, shall be specified by Protective Services.

CH1.12.2.2 Classified material shall never be removed and stored at residences for any purpose, unless specific permission is given by the Manager, Protective Services for unusual requirements or circumstances.

NOTE: No recording or transmitting devices, i.e., cameras, cell phones, etc., or other devices with digital capabilities, shall be introduced into an area housing the processing, display, or open storage of classified information. Periodic spot checks of such areas shall be conducted. Discovery of any such devices shall be considered a security violation. A formal investigation shall be conducted and the appropriate administrative/disciplinary action shall be taken.

CH1.12.2.3 Upon declaration of a major emergency or disaster, supervisors and custodians shall ensure an orderly and effective securing of classified material. If possible, without jeopardizing employee safety, classified material shall be secured in authorized storage containers or controlled access areas prior to departure.

CH1.12.2.4 When unauthorized persons are present, classified material shall be covered, turned face down, placed in security containers, or otherwise protected. Classified conversations shall also be suspended.

CH1.12.3 Use of Classified Storage Containers

CH1.12.3.1 To minimize the risk of compromise, safes which contain classified material shall not be used for storing highly desirable items such as funds, weapons, controlled drugs, precious metals, or other valuable property unless specifically approved by Protective Services.

CH1.12.3.2 Containers approved for storage of classified material shall not be relocated without prior approval from Protective Services. When a move of a security container with classified material is necessary, the custodian or cleared designated representative shall accompany the container while it is being moved.

CH1.12.3.3 Containers not being used for storage of classified material shall have an MSFC Form 1561, "No Classified Material Stored In This Container," attached to the top drawer.

CH1.12.3.4 Individual drawers of security containers shall not be labeled to show the classification level of the material stored within.

CH1.12.4 Opening, Closing, and Checking Storage Containers

CH1.12.4.1 Standard Form 702, Security Container Check Sheet, shall be posted on the outside of each container to certify the opening, closing, and checking of each security container approved for storage of classified material. A single Form 702 is permitted at the entrance to an area in which all security containers therein are opened and closed at the same time.

NOTE: During non-duty hours, or at any time a person is working alone, he/she is charged with the full responsibility for the security of the container.

CH1.12.4.2 Open security containers shall be under the direct control of a person authorized to open the container. A current list shall be maintained of the names, addresses, and phone numbers of persons having knowledge of the combination and shall be recorded on Standard Form 700, Security Container Information, and posted on the inside of the top drawer or the locking drawer/door of the security container.

CH1.12.4.3 Reversible "open-closed" or "open-locked" status signs, available through Protective Services, shall be used on each security container in which classified information is stored.

CH1.12.4.4 Security containers shall be locked when unattended. To secure the container, all doors or drawers shall be closed, and the combination dial shall be turned at least four

revolutions in the same direction and the handle pulled to ensure it is locked. Each door or drawer shall be checked to be sure that it is latched.

CH1.12.4.5 The end-of-day check shall include each room, area, or item of equipment in which classified information is stored, handled, or processed to ensure that:

a. Classified material is stored in the manner prescribed for the assigned classification level.

b. Desktops, wastebaskets, and mail trays do not contain classified material.

CH1.12.5 Changing Combinations to Security Containers

CH1.12.5.1 Combinations shall be changed:

a. The initial receipt of the container or upon assuming possession of the vault or area.

b. The relief, transfer, discharge, termination, extended hospitalization, leave of absence, suspension, or revocation of the clearance of any person who knows the combination.

c. The compromise or suspected compromise of the container or its combination, e.g., discovery that the container has been left unlocked and unattended.

CH1.12.5.2 The combinations to all vaults and all containers shall be changed by Protective Services' locksmith or other personnel authorized by Protective Services.

CH1.13 Marking Classified Accountable Material

The intent of classification markings is to make them immediately recognizable by anyone who has access to the material to show the degree of protection to be given to the information. All portions of information shall be clearly identified by the level of classification, or marked "UNCLASSIFIED." Protective Services shall provide specific guidance on marking NASA-generated classified documents.

CH1.13.1 Originator's Responsibility

The originator of classified material shall be responsible for initially stamping or marking the classification designation, authority for classification, downgrading and declassification notation, and other required security caveats on all classified material he/she originates, regardless of its physical content. The document shall be brought to Protective Services for guidance and control of any origination of classified information.

CH1.13.2 Use of Classified Document Cover Sheets

Cover sheets shall be securely attached so as to completely cover the top surface of a classified document at all times. If the document is then placed in a binder, the front and back of the binder shall also bear the classification marking. The cover sheets are:

a. TOP SECRET Cover Sheet, SF 703.

b. SECRET Cover Sheet, SF 704.

c. CONFIDENTIAL Cover Sheet, SF 705.

CH1.14 Reproduction of Classified Accountable Material

CH1.14.1 Reproduction of classified documents shall be coordinated with Protective Services. SECRET and CONFIDENTIAL material shall only be reproduced by Protective Services Document Control, or a means approved by Protective Services, and limited to the minimum quantities necessary for operational purposes.

CH1.14.2 Requests to reproduce classified material originated outside NASA that prescribes a restriction against reproduction shall be submitted to the Protective Services. The material shall not be reproduced without authorization of the originating agency or organization.

CH1.15 Destruction of Classified Accountable Material

To prevent the unnecessary accumulation of classified documents, classified accountable documents no longer required shall be returned to Classified Document Control for destruction. MSFC organizations storing classified information shall establish a program for the continuous review of classified documents for the purpose of reducing the quantity on hand.

CH1.15.1 Methods of Destruction

CH1.15.1.1 Classified material, to include classified waste, shall be destroyed beyond recognition so as to preclude reconstruction of the classified information in whole or in part. Destruction of MSFC classified material or sensitive information shall be accomplished at approved locations by disintegration, shredding, mulching, or other methods approved by Protective Services.

CH1.15.1.2 A NASA truck (mulching truck) with disintegrator is available at designated locations to receive and destroy classified, sensitive, or Privacy Act material embodied in paper products (no microfiche). Large staples, paperclips, binders, etc., shall be removed.

CH1.15.2 Preparing Material for Destruction

CH1.15.2.1 Custodians shall inventory accountable material and return inactive classified material to the CMCO for destruction. The CMCO shall prepare a Certificate of Destruction to provide an audit trail of destroyed accountable classified documents.

CH1.15.2.2 Non-accountable material, to include classified working documents or by-products shall be destroyed, beyond recognition or reconstruction, by burning, use of an approved crosscut shredder, or pulverizing. Non-accountable material does not require a destruction certificate. However, the custodian may wish to prepare one for an audit trail.

CH1.15.3 Records of Destruction

CH1.15.3.1 The CMCO shall prepare a Certificate of Destruction to accompany accountable classified material. The original destruction certificate shall be retained by Protective Services.

CH1.15.3.2 TOP SECRET material shall be personally destroyed by the TOP SECRET Control Officer (TSCO) or alternate in the presence of a properly cleared witness. The TSCO shall maintain TOP SECRET accountability and destruction records for a minimum of 5 years.

CH1.16 Reporting Compromises of Classified information

CH1.16.1 Employees or associated contractors who suspect a compromise of classified information or other related security incident shall immediately report the observation to Protective Services, immediate supervisor, office chief, or higher authority.

CH1.16.2 Immediate action shall be taken to regain the custody of lost classified documents or material. However, as a minimum, appropriate action shall be taken by Protective Services and the affected organization to identify the source and reason for the compromise, and to take necessary action to ensure that further compromise does not occur.

CH1.16.3 If the Center is not the originating organization of the potentially compromised information, the office of primary responsibility shall be notified, as well as NASA Headquarters security management.

CH1.17 Preliminary Inquiries and Formal Investigations

CH1.17.1 Protective Services shall initiate a preliminary inquiry, formal investigation, and/or a damage assessment as necessary, to determine the circumstances and seriousness of a compromise or security incident involving classified information.

CH1.17.2 A written investigative report of findings, conclusions, and recommendations shall be forwarded to the Center Director and appropriate organization for review and corrective actions, as necessary. A reply indicating the actions taken shall be returned to Protective Services by the affected organization.

CH1.18 Administratively Controlled Information (ACI) (See NPR 1620.1 at http://nodis3.gsfc.nasa.gov for full details):

CH1.18.1 NASA Headquarters has determined that official information and material, of a sensitive but unclassified nature, which does not contain national security information (and therefore cannot be classified) shall be Administratively Controlled Information (ACI), and shall be protected against inappropriate disclosure. (See NPR 1620.1 for detailed information and guidance). Within NASA such information has previously been designated "FOR OFFICIAL USE ONLY." This designation has been changed to ACI for clarity and to more accurately describe the status of information to be protected. (See "Document Content" "1. Definitions" for definition of ACI and Sensitive Information/Material, this MPR).

CH1.18.2 The "FOR OFFICIAL USE ONLY" (FOUO) designation shall still be applied to material, reports, or analysis of agencies or departments outside of NASA whose authorities are derived from other sources. This includes COMSEC Material Reports because they are handled and transferred between all Government agencies. When such information is copied or distributed within NASA, it shall still carry the "FOR OFFICIAL USE ONLY" designation and bear an FOUO cover sheet.

CH1.18.3 The failure to sufficiently identify material that requires protection from disclosure may result in damage to official relationships, monetary or other loss to individuals or firms, embarrassment to NASA, or criminal prosecution.

CH1.18.4 The MSFC employee who originates, or the organization procuring contractor data, shall review material for possible designation as ACI prior to use. Criteria of at least one of the following shall be met:

a. Information Protected by Statute – (e.g., Export Administration Act; Arms Export Control Act; Space Act).

b. Information the originator determines to be unusually sensitive.

c. Information Exempt from the Freedom of Information Act (FOIA), including the following:

(1) Internal Personnel Rules/Practices
(2) Trade Secrets/Commercial/Financial
(3) Inter/Intra-Agency Memos & Letters
(4) Personnel and Medical Files
(5) Investigative Records
(6) Financial Institution Information
(7) Geological/Geophysical
(8) Maps/Documents of underground utilities
(9) Drawings/specifications for Mission Essential Infrastructure (MEI) or other assets
(10) Mission specific security plans

(11) Emergency Contingency plans

CH1.18.5 Information shall not be marked or designated as ACI if it does not meet the criteria in 1.17.4 above and in NPR 1620.1.

CH1.18.6 Those originators or procuring organizations who designate information as ACI shall be responsible for continued review and removal/decontrol of the information when the necessity no longer exists.

CH1.18.7 Marking

CH1.18.7.1 Information designated ACI shall be marked at the top and bottom of each page; e.g., "Administratively Controlled Information – NASA Sensitive, or Proprietary, or Investigative Records, etc."

CH1.18.7.2 For those documents that already have cover sheets and marking for protection purposes (Federal Acquisition Regulations (FAR), FOUO, Export Control, FOIA), ACI marking is not required; however, they shall be protected per ACI guidelines.

CH1.18.8 Safeguards

ACI information shall be safeguarded as follows:

- Attended when in use
- Access limited to those with "need to know"
- Limit number of hard copies
- Stored under lock and key when unattended (locked desk, locked office, locked cabinet, or locked office suite)
- ACI cover sheet (NF 1686) when transmitted on or off Center (optional for FAR, FOUO, Export Control, FOIA, but physical protection is the same as for ACI)
- Stored on secure server with appropriate markings/warnings (contact the Office of Chief Information Officer to see what your secure server is)
- No further dissemination of ACI without approval
- Encrypted e-mail transmission
- Transmitted by Secure Fax or person to person tracking on unclassified fax
- Destroy by shredding, burning, removing from IT systems

CH1.18.9 Violations and Sanctions

CH1.18.9.1 Individuals shall be subject to administrative sanctions if they disclose information designated ACI. Sanctions include, but are not limited to, a warning notice, admonition, reprimand, suspension without pay, forfeiture of pay, removal or discharge.

CH1.18.9.2 Such sanctions shall be imposed, as appropriate, upon any person determined to be responsible for a violation of disclosure in accordance with applicable law and regulations, regardless of office or level of employment.

CH1.19 For more detail on Export Control procedures, see MPD 2190.1, "MSFC Export Control Program."

Chapter 2

CLASSIFICATION MANAGEMENT

CH2.1 Responsibilities

CH2.1.1 Protective Services. When a program or paper is determined to require original classification, Protective Services shall:

CH2.1.1.1 Assist in the development and issuance of security classification guidelines.

CH2.1.1.2 Interpret and provide NASA policy on security classification guidance. Obtain original classification from the NASA Headquarters' Original Classification Officer.

CH2.1.1.3 Coordinate and evaluate technical input regarding security classification matters, provide guidance on handling classified material, and ensure a continuing review of classified information to facilitate declassification or downgrading actions.

CH2.1.2 The Director, Procurement Office shall:

Upon notification that a contract is subject to the receipt or use of classified information, take the necessary actions to introduce contractually (during the solicitation and contract award) the security instructions by means of a DD Form 254, Contract Security Classification Specification, and other security classification instructions, as appropriate. (An original 254 shall be issued by the Protective Services when the contract is let).

CH2.2 Conditions for Security Classification

CH2.2.1 A security classification determination shall occur when the conditions of the classification Executive Order are met.

CH2.2.2 Information shall not be classified to conceal a violation of law, inefficiency, or administrative error; to prevent embarrassment to a person, an organization, or an agency; to restrain trade or contract competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

CH2.3 Classification Designations

As a precondition to classifying information, the originator shall determine that the unauthorized disclosure of the information could be expected to cause damage to national security. There are three security classification designations used to reflect the varying degrees of damage that could occur to national security if the information were compromised:

CH2.3.1 TOP SECRET – information where the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

CH2.3.2 SECRET – information where the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

CH2.3.3 CONFIDENTIAL – information where the unauthorized disclosure could reasonably be expected to cause damage to the national security.

CH2.4 Duration of Classification

CH2.4.1 Classified information shall be classified only as long as required by national security considerations. Normally, the material shall remain classified for a determined period of time based on the loss of its sensitivity with the passage of time or upon occurrence of an event identified in the information; e.g., completion of a classified test. Executive Order (EO) 12958 requires an attempt to set a specific date or event within 10 years. When exempt from the 10-year rule, the maximum classified life span should be 25 years unless it is Restricted Data or another rare exception.

CH2.4.2 The predetermined date of declassification shall be identified on the face of the document. Any classification changes shall be coordinated with Protective Services.

CH2.4.3 The NASA appointed original classification authority may extend the duration of classification for MSFC-originated information, if all known holders of the information are notified before the declassification date.

CH2.5 Declassifying and Downgrading

CH2.5.1 When a document qualifies for downgrading, the accountable custodian shall conduct a systematic review of the dates or events specifying the downgrading or declassification of classified information in his/her custody. When an event has occurred or date for declassification has passed, the custodian shall contact Protective Services for assistance in downgrading or declassifying the information in question.

CH2.5.2 Declassifying a classified document does not automatically allow the document to be released to the public. Accordingly, request to process public disclosure of "previously classified" information shall be submitted to Protective Services for review by the CMCO and Export Control.

CH2.6 Derivative Classification

CH2.6.1 Derivative classification is a determination that certain MSFC-originated information is, in substance, the same as existing information that is currently classified. Therefore, such classification shall be applied.

CH2.6.2 MSFC employees exercising derivative classification shall take care to ensure that the paraphrasing, restating, or summarizing of previously classified information has not removed all or part of the basis for classification. Protective Services can assist in this process.

CH2.6.3 Originators of classified information shall respect the original classification authority's decision, verify the information's current level of classification when practical, and carry forward to a derivatively classified document the assigned date or event for declassification assistance in applying derivative classification to MSFC-originated documents.

CH2.7 Security Classification Guide (SCG)

CH2.7.1 A Security Classification Guide shall be developed, as appropriate, and issued by the original classification authority to employees involved in classified systems, programs, plans, or projects to ensure an accurate and consistent classification of information. An SCG shall precisely identify the functional matter that is to be protected, at what level, and for how long. The SCG serves as the classification authority for cleared employees to classify the information.

CH2.7.2 A DD Form 254, which sets forth the classification specification or cites the classification guidance documents, SCG, shall be issued to associated contractors involved in classified projects to provide accurate and consistent classification guidance in performance of a contract requiring classified activity.

CH2.8 Challenging a Security Classification

Employees who have substantial reason to believe that information is classified improperly or unnecessarily shall contact the Security Classification Officer for a classification review and determination. The information shall be safeguarded in the manner prescribed at the classification level initially assigned, pending the Security Classification Officer's final determination.

CH2.9 Notification of Changes in Declassification Or Downgrading

A notification shall be sent to all known holders to whom the information was originally transmitted when a declassification action is directed earlier than originally scheduled, when the duration of classification is extended, or when it is determined to regrade the information. The notification shall specify the marking action to take, the authority directing the action, and the effective date.

CH2.10 Marking Classified Documents

CH2.10.1 The person generating a classified document shall be responsible for designating it with the proper classification. Contact the Security Classification Officer for specific guidance on the proper marking of different forms of classified information or material.

CH2.10.2 The physical marking, notation, or other means to identify classification information shall serve to warn the holder about the classification of information involved, to indicate the degree of protection required for the information, and to facilitate the timely declassification or downgrading of information.

CH2.10.3 If the material does not lend itself to marking, classification and other associated security markings shall be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal, or similar device on classified material other than paper copies of documents. These markings shall be included on the container of such material, when possible. The following standard form stickers may be ordered: SF 708, CONFIDENTIAL; SF 707, SECRET; SF 706, TOP SECRET; SF 712, SCI; and SF 709, CLASSIFIED.

Chapter 3

SECURITY EDUCATION AND TRAINING PROGRAM

CH3.1 Standard Briefings

CH3.1.1 Security Orientation Briefings

CH3.1.1.1 Protective Services, in cooperation with supervisors, has an obligation to ensure all MSFC and appropriate contractor employees receive the necessary orientation and instructional training.

CH3.1.1.2 Employees, both cleared and uncleared, shall be given training on the policies and procedures for effectively safeguarding information and critical NASA resources from theft, loss, or damage. A cooperative training effort between the employee, supervisor, and Protective Services should result in the employee having a good working knowledge of relevant security policies.

CH3.1.1.3 Supervisors shall ensure an initial security orientation briefing is coordinated and conducted by Protective Services for new hires and employees who enter new work assignments requiring knowledge of additional security requirements. A detailed security briefing shall be given within 30 days of an employee being granted a security clearance, unless this requirement is waived by the Manager, Protective Services.

CH3.1.2 Security Information Training

In addition to the training outlined in paragraph 3.3, Protective Services shall issue Center-wide messages, conduct SOLAR training, conduct Community Resource Officer briefings, or issue Memorandums to inform or remind employees of current or changing security procedures and guidelines.

CH3.1.3 Termination Briefings

CH3.1.3.1 Employees shall read, understand, and complete NASA Form 839, Security Termination Statement, to acknowledge an ongoing responsibility not to discuss or reveal classified NASA information without prior authorization by NASA. By signing, employees are giving assurance that all classified material has been returned, and are acknowledging their understanding of penalties for gathering, transmitting, or losing classified information.

CH3.1.3.2 A record copy of the NASA Form 839 shall be retained by Protective Services, with a copy provided to the employee upon request. If circumstances prevent an employee from appearing in person, Protective Services shall request assistance from the appropriate supervisor in accomplishing the termination briefing and recovering the employee's badge, keys, decals, etc.

CH3.2 Special Briefings

CH3.2.1 Document Control Station Officer (DCSO) Briefings

Protective Services, CMCO, shall conduct initial and annual refresher training for employees appointed as Classified Information Custodians.

CH3.2.2 Communications Security (COMSEC) Officer Briefings

The MSFC COMSEC Account Manager shall conduct initial training for employees appointed as COMSEC officers which grants authorization for access to U.S. cryptographic information. The COMSEC user shall read, understand, and sign a Cryptographic Access briefing prior to gaining access to COMSEC information.

CH3.2.3 COR/COTR Security Briefing

Protective Services shall provide security education briefings for those MSFC personnel who are responsible for oversight of MSFC contracts.

CH3.24 Contractor Security Personnel Briefings

Protective Services shall provide security briefings for contractor facility security personnel.

CH3.2.5 In addition to the above briefings Source Evaluation Board, Counterintelligence, Foreign Travel, and Foreign Escort briefings shall be conducted on a periodic and as-needed basis.

Chapter 4

VISITOR CONTROL

CH4.1 MSFC Visitor Control:

Visitor control is needed for the protection of installation and property, personnel, and classified or sensitive/unclassified information.

CH4.2 Responsibilities

CH4.2.1 Protective Services shall:

CH4.2.1.1 Provide guidance to employees when submitting a Visit Notification.

CH4.2.1.2 Review visit requests (incoming and outgoing) to ensure that they are complete and that approval of necessary organizations has been obtained.

CH4.2.1.3 Upon approval of a visit, distribute (mail or fax) copies or telephonically advise the office to be visited.

CH4.2.1.4 Verify personnel security clearances, as required, for access to classified information.

CH4.2.2 The Identification and Registration Section shall:

CH4.2.2.1 Issue and control all visitor badges and maintain a record of all visitors, to include full name, citizenship, organization represented, person to be visited, clearance status, and date.

CH4.2.2.2 Verify the identity of all visitors ages 16 and older and issue the appropriate visitor identification badge. Two forms of identification are required; one shall be a photo ID and one shall be a government form of identification. (A driver's license or other government photo ID may double as a government ID, but a second identification is still required.) Business cards are not acceptable.

CH4.3 Outgoing Visits

MSFC employees requesting to visit another Government Agency or contractor facility, in connection with the receipt, release or discussion of classified information, shall complete MSFC Form 2548, Visit Notification, as required. The request shall be submitted to Protective Services at least 5 workdays prior to the projected date of visit. Incomplete visit requests shall be returned to the originator. In an emergency, Protective Services may notify the facility to be visited by telephone, provided written confirmation follows. Protective Services shall fax or mail the visit notification to the appropriate Security Office.

CH4.4 Visits to Other NASA Installations

Formal visit notification is not required for MSFC civil service employees visiting another NASA installation unless otherwise specified. Likewise, visits to MSFC by civil service employees of other NASA installations do not require formal notification and approval. Verification of employment and personnel security clearances shall be done by a phone call to the respective Center security office.

CH4.5 Incoming Visits

CH4.5.1 Visits General

CH4.5.1.1 All visitors shall be entered into the Visitor Management System for gate access by 2 p.m. on the day prior to the visit. If they are not entered into the system, a badged sponsor shall meet the visitor at the gate and escort them on Center.

CH4.5.1.2 Arrangements for visits by US citizens should be made 3 to 5 working days in advance of the visit with the MSFC sponsor in order to coordinate badging.

CH4.5.1.3 Vendors, suppliers, utility service representatives, and construction contractor employees who are here for 30 days or less shall be issued visitor badges by I&R that have a badge expiration date clearly marked on the badge.

CH4.5.1.4 Visitors not under a formal agreement or contract shall be issued a visitor badge for 1 day only, unless otherwise approved by Protective Services.

CH4.5.1.5 Visitors shall be escorted after hours unless unescorted after hour's access is approved in advance by Protective Services.

CH4.5.1.6 Visitor badges shall be issued for 30 days at a time with a maximum of two 30 day visitor badges per year. Additionally, requests shall be fully justified and approved by Protective Services, and shall require a favorable background investigation.

CH4.5.2 Classified Visits

CH4.5.2.1 Incoming visitors who require access to classified information while at MSFC shall submit a Visit Notification to Protective Services for approval prior to the visit.

CH4.5.2.2 Protective Services approval of the visit constitutes authority to disclose classified information within the limitations of the established visitor clearance. The person being visited shall be responsible for controlling access to information consistent with the level of security clearance and the purpose of the visit. Contact Protective Services for confirmation of security clearance, as necessary.

CH4.5.3 Visits by Foreign Nationals

See MPR 1371.1, “Procedural Requirements for Processing Foreign Visitor Requests.”

Chapter 5

INDUSTRIAL SECURITY PROGRAM

CH5.1 Reference

CH5.1.1 DOD 5220.22M, "National Industrial Security Program Operating Program," (NISPOM)

CH5.1.2 NPR 1620.1, "Security Procedures and Guidelines," chapter on Industrial Security

CH5.2 Responsibilities

CH5.2.1 The Procurement Officer shall:

CH5.2.1.1 Adhere to the guidelines of NPR 1620.1.

CH5.2.1.2 Ensure the identification and inclusion of all necessary security requirements and adherence to MPR 1600.1 and NPR 1620.1 guidelines when requesting bids or quotations, negotiating or awarding a contract with access requirements for National Security Information, or bearing responsibility for the performance of such a contract.

CH5.2.2 Protective Services shall:

CH5.2.2.1 Provide oversight of industrial security matters involving on-site and component facility MSFC contracts, and coordinate security matters involving off-site contractors with the Defense Security Service.

CH5.2.2.2 Redelegate authority, by means of the DD Form 254, to the Defense Security Service for security cognizance over off-site MSFC contractors in performance of such contracts.

CH5.2.2.3 Periodically conduct a security evaluation of on-site MSFC contractor operations to ensure compliance with pertinent security requirements, and that classified material is adequately safeguarded.

CH5.2.2.4 Provide advice, assistance, and training for proper protection, storage, transmittal, and destruction of classified materials.

CH5.2.2.5 Advise the Procurement Office on unique security requirements related to a specific contract.

CH5.2.2.6 Coordinate the completion of a DD Form 254 with the Contracting Officer (CO), and the Contracting Officer's Technical Representative (COTR), and distribute appropriately.

CH5.2.2.7 Manager, Protective Services shall redelegate a security specialist to serve as the Center Security Classification Officer responsible for informing the Center Director of significant actions, problems, or other matters related to security classification and to serve as the signature authority for DD Form 254.

CH5.2.2.8 Designate and obtain approval on all on-site controlled access areas, as necessary, to safeguard classified material.

CH5.2.3 The Defense Security Service (DSS) shall:

CH5.2.3.1 Serve as the cognizant security office for supervision and inspection of such contracts executed by MSFC and performed at off-site contractor facilities.

CH5.2.3.2 Issue a contractor's facility security clearance (FCL) and personnel security clearances, as required in performance of MSFC contracts.

CH5.2.4 The DSS Operations Center shall:

Conduct contractor personnel security investigations and issues an appropriate security clearance. DSS Operations Center may deny, suspend, or revoke a contractor employee's personnel security clearance for cause.

CH5.2.5 Employees shall:

Ensure that classified information in their possession, or to which they have access, is properly safeguarded and disclosed only in accordance with the established requirements of this handbook, applicable security classification guides, or other appropriate directives.

CH5.2.6 Contract Initiating Office (IO) shall:

CH5.2.6.1 Make an initial determination as to whether a contractor or prospective contractor shall require access to, generation of, or storage of classified information. If so, advise the MSFC contracting officer or designated representative of the determination. The IO preparing the MSFC Form 404, Purchase Request, shall indicate whether or not the contractor shall require access to, or shall be generating, classified information. Protective Services shall assist the IO in verifying the facility security clearance.

CH5.2.6.2 Coordinate with Protective Services in the preparation of a DD Form 254, Contract Security Classification Specification, for each contract or procurement that requires access to classified information, data, or material.

CH5.2.6.3 Recommend contract security-related requirements and provide technical guidance for protection of classified data or material relative to the proposed contract.

CH5.2.6.4 Ensure the following information has been considered or included in contract documents accompanying the MSFC 404 prior to release of the RFP:

a. Specific program or project affected.

b. Date which classified access or information required.

c. Expected duration of the contract.

d. Request for Defense Technical Information Center (DTIC) services, as required.

e. Whether automated data processing or Department of Energy restricted data are involved.

CH5.2.6.5 Recommend technical and security classification guidance for successful completion of the contract.

CH5.2.6.6 Review the DD Form 254 on a continuing basis to ensure it is current.

CH5.2.6.7 Immediately advise Protective Services and Procurement Office of necessary contract changes.

CH5.2.6.8 Conduct an annual review of each DD Form 254 prior to contract anniversary date. The contract technical monitor shall notify the Procurement Officer and Security Classification Officer of any proposed changes to the security classification specification.

CH5.2.7 Contracting Officers and Representatives shall:

CH5.2.7.1 Incorporate appropriate security specifications into each RFP and contract.

CH5.2.7.2 Ensure a DD Form 254 identifies special security requirements and has been coordinated and approved by Protective Services prior to release of the RFP of other contract request.

CH5.2.7.3 Request Protective Services assistance, as required, during Source Evaluation Board (SEB) activity in which classified information is required in performance.

CH5.2.7.4 Provide the Security Classification Officer a copy of all amendments and contract modifications which extend, modify, or terminate the performance of a classified contract.

CH5.3 Types of Clearances

A facility security clearance shall be granted by the cognizant DSS Regional Office to a contractor facility when, in the performance of a NASA contract, access to classified national security information is required.

CH5.4 Personnel Security Clearances

CH5.4.1 The cognizant security office shall notify the Facility Security Officer (FSO) when a favorable personnel security clearance has been granted. Protective Services shall receive notice of contractor personnel security clearances by the Facility Security Officer via individual visit requests. These shall include all pertinent personnel security clearance data and should be sent to the MSFC Visitor Control prior to a visit for the purpose of discussing classified information. Further, they shall be updated annually.

CH5.4.2 Contractors shall be employed or retained in a position that requires a personnel security clearance only when it is consistent with the interests of national security.

CH5.5 Reporting Security Incidents or Compromises

MSFC contractor and civil service employees who suspect a security incident or compromise of classified information has occurred shall immediately report the matter to Protective Services for investigation. Off-site contractor employees shall immediately report suspected incidents or compromises to the contractor Facility Security Officer (FSO), who shall take appropriate action in accordance with the NISPOM.

CH5.6 Redstone Scientific Information Center (RSIC)

The Redstone Scientific Information Center provides for approved access to information of a scientific and technical nature for use in support of MSFC contracts and U.S. Army contracts. The contractor's security officer shall request this service on the RSIC Patron Card, and obtain the signature of Protective Services before a contractor is allowed access to RSIC.

Chapter 6

PERSONNEL SECURITY PROGRAM

CH6.1 General

CH6.1.1 Initiating, investigating, and maintaining personnel security clearances demands a great expenditure of both dollars and time. Supervisors shall use NASA Form 1630, "Request for Access to Classified National Security Information," to judiciously nominate candidates to fill the sensitive positions in their areas. The clearance process is intended to eliminate employees whose trustworthiness, based on previous behavior, may be questionable.

CH6.1.2 The focus of personnel clearability relates directly to the requirements for access to classified information, and whether the granting or continuance of a personnel security clearance is consistent with the interests of national security. Protective Services shall periodically evaluate employees working in designated sensitive positions to significantly reduce the possible insider threat.

CH6.1.3 An employee in a position that requires access to classified NASA information shall be subject to a personnel suitability determination. Any information that reflects adversely on the integrity or character of an employee and suggests that his or her ability to safeguard classified information may be impaired shall be reported to Protective Services.

CH6.1.4 The necessity for a person to have a security clearance is based, in part, on position sensitivity and provides a basis for ensuring that employment of the employee is clearly consistent with the interests of national security.

CH6.2 Responsibilities

CH6.2.1 Protective Services shall:

CH6.2.1.1 Request a review and revalidation of Civil Service security clearances annually by calling for new NASA Forms 1630 for each employee clearance needed.

CH6.2.1.2 Appoint a trained and certified Personnel Security Specialist to review, and process personnel security investigations on MSFC employees requiring access to classified information.

CH6.2.1.3 Review the NASA Form 1630 and initiate an investigation, if required.

CH6.2.1.4 Provide guidance and detailed instructions to nominated employees for completing personnel security investigation forms. The investigation forms shall be prepared by the employee being investigated.

CH6.2.1.5 After completion of the investigation and adjudicative process, notify the employee of results. If the clearance was granted, Protective Services shall schedule a cleared employee briefing with the employee.

CH6.2.1.6 Maintain clearance records in employee personnel security files.

CH6.2.1.7 Ensure that the Center Director is kept fully informed of significant actions, problems, or other matters of substance related to the authority to administer the MSFC Personnel Security Program.

CH6.2.2 Managers and Supervisors shall:

CH6.2.2.1 Exercise judicious restraint when nominating candidates to fill sensitive positions. Submit candidates only when there is a valid requirement for access to classified information or unclassified/sensitive activity in connection with a NASA project.

CH6.2.2.2 Confirm that prospective employees understand and accept the responsibilities and requirements of handling classified information prior to submitting their names for investigation.

CH6.2.2.3 Justify and nominate candidates who shall occupy a sensitive position requiring access to classified information using the NASA Form 1630.

CH6.2.2.4 Notify Protective Services when a cleared employee no longer requires access to classified information and does not anticipate a requirement for access in the near future.

CH6.2.2.5 Upon notification of unfavorable information, take immediate action to preclude continued access to classified information.

CH6.2.3 Employees Subject to Investigation shall:

CH6.2.3.1 Upon request, properly complete the standard forms in a within 10 working days to assist Protective Services in determining eligibility for a personnel security clearance.

CH6.2.3.2 Adhere to established security procedures. A failure or unwillingness to follow security requirements shall serve as the basis to deny, suspend, or revoke a security clearance.

CH6.2.3.3 Attend an initial security orientation briefing which shall provide a basic understanding of the security requirements for access and handling of classified material and refresher training, as required.

CH6.3 Administrative Withdrawals/Downgrading

CH6.3.1 A personnel security clearance shall be administratively withdrawn when an employee no longer requires access to classified information and a need for access is not anticipated within

one year; upon termination of employment; and at the beginning of a leave of absence for an indefinite period.

CH6.3.2 Employees shall be notified that the clearance is being terminated and that in no way does this action reflect adversely on the employee or on future eligibility for a personnel security clearance.

Chapter 7

MISSION CRITICAL SPACE SYSTEMS PERSONNEL RELIABILITY PROGRAM

CH7.1 General

The MSFC Mission Critical Space Systems Personnel Reliability Program (MCSSPRP) applies to any position requiring its incumbent to have physical access to the Space Transportation System (STS) vehicle, or mission-critical command capability through the Launch Processing System or the Mission Control Center. This program also applies to other positions where the concerned program/project office determines that faulty, negligent, or malicious actions could result in a program contingency.

CH7.2 Responsibilities

CH7.2.1 The Associate Director, MSFC shall:

CH7.2.1.1 Review recommended action of the Review/Certification Board.

CH7.2.1.2 Render final decision on appeals of personnel certifications to mission-critical positions denied by the MSFC Certifying Officer.

CH7.2.2 Managers/Directors shall:

CH7.2.2.1 Designate mission-critical positions and nominees thereto and notify Protective Services and their designees via memorandum. The number of positions designated mission-critical shall be kept to an absolute minimum and identified sufficiently in advance of need. Action taken within this responsibility, with respect to MSFC civil service personnel and contractors is subject to the concurrence of the director/manager of the parent organization to which the nominee is assigned.

CH7.2.2.2 Provide rationale for each position designated mission-critical and attest that the nominees, as specifically applied to critical duties, are reliable, dependable, trustworthy, and technically qualified.

CH7.2.2.3 Nominate civil service and/or contractor personnel for MCSSPRP certification by Directorate level memorandum to Protective Services.

CH7.2.2.4 Notify their contractors of the certification action taken on contractor employees.

CH7.2.2.5 Continually evaluate an employee's suitability for access to mission-critical positions. Monitor the performance, attitude, and behavior of a certified employee and

immediately report profile deviations, unusual behavior, or other potentially significant adverse information to Protective Services for evaluation.

CH7.2.2.6 Notify Protective Services when a certified employee no longer requires access to mission-critical areas and does not anticipate a requirement for access in the near future.

CH7.2.3 Manager, Protective Services shall:

CH7.2.3.1 Be responsible for the operational management of the MCSS Personnel Reliability Program by certifying that eligible candidates meet all requirements.

CH7.2.3.2 Ensure that the Center Director is kept fully informed of significant actions, problems, or other matters of substance relating to the exercise of authority to administer the MSFC PRP.

CH7.2.3.3 Appoint a trained Security Specialist to review and process nominated employees.

CH7.2.4 Director, Procurement Office, shall:

Include a clause in the contract requiring compliance with this handbook when advised by the organizational or program manager that his/her contractors are required to perform in mission-critical positions.

CH7.2.5 Review/Certification Board shall:

CH7.2.5.1 Review all appeals of denial of personnel by the MSFC Certifying Officer and recommend action to the Associate Director, MSFC.

CH7.2.5.2 Notify the appellant of the final decision, with supporting rationale, and furnish a copy of the notification to the MSFC Certifying Officer.

CH7.2.6 Protective Services shall:

CH7.2.6.1 Upon receipt of memorandum requesting PRP certification, process civil service nominees for mission-critical positions as follows:

a. Review personnel security files and initiate an investigation, if necessary.

b. Review the Official Personnel Folder.

c. Request the Medical Center Director to review the medical files for any medical information that could adversely affect the nominee's capability to properly perform the duties of a mission-critical position.

d. Review Office of Inspector General case files.

CH7.2.6.2 Process contractor employee nominees for mission-critical assignments as follows:

a. Request the contractor security officer to certify a review of the company security, medical, and personnel files and furnish any information that might adversely affect the nominee's capability to properly perform the duties of a mission-critical position; or request the contractor nominee to complete an SF 85-P-S if company information cannot be obtained.

b. Review of Office of Inspector General case files.

c. Initiate an investigation, if necessary.

CH7.2.6.3 Deny certification of a nominee if eligibility requirements are not met and provide written notification to the nominee that includes the rationale for the denial. The nominee shall also be advised that the decision may be appealed to the Review/Certification Board within 10 working days, and that the nominee may personally appear before the board to present his/her appeal.

CH7.2.6.4 Furnish the Review/Certification Board (RCB), in all cases of appeals, all documentation for the case, as requested by the RCB.

CH7.2.6.5 Administer the review by competent medical authority of medical records for indications of any significant physical or mental impairment, character disorder, or aberrant behavior that might affect reliable performance of duties, defining relevant medical standards for such duties. Ensure the conduct of further examinations, as recommended, if information is insufficient.

CH7.2.6.6 Ensure that Management is kept fully informed of significant actions, problems, or other matters of substance relating to the exercise of authority to administer the MSFC Personnel Reliability Program.

CH7.2.7 Employees Subject to investigation shall:

CH7.2.7.1 Upon request by Protective Services, complete the investigation forms within 2 weeks to assist in determining eligibility for PRP certification. Return the completed forms to Protective Services for review and processing.

CH7.2.7.2 Adhere to established security procedures. A failure or unwillingness to follow security requirements shall serve as the basis to deny, suspend, or revoke certification.

CH7.2.7.3 Attend an initial KSC security/safety orientation that provides a basic understanding of the requirements for working in a mission-critical position.

CH7.3 Determination of Acceptability for Mission-Critical Positions

Determination of acceptability for assignments to mission-critical positions shall be made on the basis of the following criteria:

CH7.3.1 Ability to perform mission-critical duties as evidenced by performance during training, simulations, and on the job performance.

CH7.3.2 Medical evaluation of the individual to ensure health is adequate for reliable performance of mission-critical duties. The medical evaluation by competent medical authority may be made by:

a. Medical history and records that are sufficiently comprehensive and current for the purpose; or

b. An appropriate medical examination.

CH7.3.3 Verification of the existence of a current personnel security clearance at the level commensurate with the classification of the information required in the position.

CH7.3.4 A review of the results of a National Agency Check (including a check of the FBI fingerprint records) completed within the past five years, with a new National Agency Check to be initiated every five years as long as the individual remains in the program. When the NAC indicates that a more extensive investigation has been completed, the results of that investigation shall also be reviewed.

CH7.3.5 Local Agency checks, as appropriate.

CH7.4 MSFC Review/Certification Board

CH7.4.1 The function of the MSFC Review/Certification Board is to review, on a case-by-case basis, the appeal of an employee (civil servant or contractor) denied certification by the MSFC Certifying Official to fill a position designated mission-critical. The review shall include the personal appearance of the appellant before the board, if the appellant so desires.

CH7.4.2 The board shall report its findings, with recommendations to the Associate Director, MSFC, for final decision.

CH7.4.3 The board shall consist of a chairperson, executive secretary, and a minimum of three members. Board membership shall be composed of management officials as follows:

a. Chairperson – Director, Center Operations

b. Executive Secretary – Director, Human Resources

c. Members:

(1) Space Shuttle Projects

(2) Safety and Mission Assurance

(3) Organization which nominated the individual

(4) Management representative of the employee's immediate organization

(5) Management representative of the prime contractor organization (when person being evaluated is a contractor employee)

d. Advisor – Chief Counsel or Designee

CH7.5 Reporting Requirements

Supervisors shall ensure the accuracy and confidentiality of reports regarding the trustworthiness of any MSFC employee. Reports of adverse actions or behavior shall be made to Protective Services, as soon as practical.

Chapter 8

CONTROLLED ACCESS AREA

CH8.1 Establishing and Maintaining Controlled Access Areas

CH8.1.1 Controlled access areas shall be identified and categorized by the Manager, Protective Services, or component installation representative, and established in writing by the Center Director, to provide protection against unauthorized access to classified material, critical hardware/software, or unclassified/sensitive property or information essential to accomplishing the MSFC mission.

CH8.1.2 To ensure the required degree of security, prescribed personnel security measures shall be taken to ensure the reliability of personnel authorized for unescorted access to designated areas. Areas designated as controlled areas shall have signs posted at all entrances.

CH8.1.3 The required security measures and internal procedures for controlled access areas shall be established by Protective Services. The measures applied to each category of controlled access area shall vary according to the sensitivity of the assets being protected and the vulnerability to unauthorized access and compromise.

CH8.1.4 Protective Services shall be informed immediately when the requirements for an area are no longer necessary.

CH8.2 Penalties for Violating Requirements

A violation of an order involving a controlled access area may be subject to prosecution under 18 U.S.C. 799, which provides penalties for a fine of not more than $5,000, or imprisonment for not more than one year, or both.

CH8.3 Types of Controlled Access Areas

CH8.3.1 Restricted Area. Restricted areas shall be designated and marked at each entrance when special security measures are taken to safeguard and control access. Restricted areas provide security for critical NASA resources, property, and hazardous materials, and protect vital mission operations.

CH8.3.2 Limited Area. Shall be designated and marked at each entrance. Limited Areas provide security for classified material or unclassified property warranting special protection. Area construction specifications or modifications may apply.

CH8.3.3 Closed Area. Closed areas are designated and marked at each entrance when special security measures are taken to safeguard classified material where entry to the area would

provide immediate visible or audible access. Area construction specifications or modifications may apply.

CH8.4 Access to Controlled Access Areas

CH8.4.1 Controlled access areas shall be separated from adjacent areas by physical barriers. Access to controlled access areas shall be restricted to the minimum number of persons required to conduct operations.

CH8.4.2 For automated access, an MSFC Form 3981(electronic), Marshall Access Control System (MACS) Access Request Form, shall be completed and submitted by the appropriate area manager, authorizing access to specific controlled access areas.

CH8.4.3 Employees approved for unescorted access by the area manager or designee shall be entered into the MACS database.

CH8.4.4 Access to a controlled access area not controlled by card readers shall be controlled by locking devices, personal identification numbers (PINs), and an authenticated access list prepared and maintained by the area manager or designee. The personnel security clearance level shall be validated by Protective Services prior to gaining access to Closed Areas.

CH8.4.5 Employees requiring access to a controlled access area, but not requiring access to classified information, shall complete a National Agency Check (NAC) prior to gaining access. The employee shall remain under the escort of a NASA or NASA contractor employee until a NAC has been successfully completed. Access approval by the designated area manager shall be required.

CH8.4.6 To enter a closed area, individuals shall have a need-to-know, and a security clearance equal to the classification of the material in the area.

CH8.5 Responsibilities

CH8.5.1 Protective Services shall:

CH8.5.1.1 Initiate an appropriate personnel investigation on an employee nominated for unescorted access when an investigation has not been adjudicated by NASA within the past 5 years. Protective Services shall conduct further investigations, as required.

CH8.5.1.2 Authorize unescorted access upon the determination that the investigation has been satisfactorily completed. Notify employees whose access is denied due to an unsatisfactory investigation based on established adjudication criteria. The notification shall be submitted in writing within 10 working days. The notification shall advise the employee of the basis for the decision and of the appeal process. A written appeal by the individual shall be submitted to a Review/Certification Board within 10 working days of receipt of notification.

CH8.5.1.3 Notify the area manager of all determinations.

CH8.5.2 The Manager, Protective Services shall:

CH8.5.2.1 Advise managers, as required, on controlled access area matters.

CH8.5.2.2 Concur with the denial of unescorted access.

CH8.5.2.3 Furnish the Review/Certification Board documentation for each particular case including the specific reason for the denial of access, present the case to the board, and provide other support as requested.

CH8.5.2.4 Notify the designated area manager in writing of all access determinations within 10 working days.

CH8.5.3 The Area Manager shall:

CH8.5.3.1 Be designated by the director/manager who controls the controlled access area designated by the Center Director.

CH8.5.3.2 Apply concentrated management effort to ensure the physical security of the controlled access area.

CH8.5.3.3 Review the results of physical security surveys, take corrective action on cited deficiencies, and report the action to Protective Services.

CH8.5.3.4 Authorize unescorted and escorted access (based upon completed security review) for employees and visitors to controlled access areas under their control. Ensure that visitors are properly escorted.

CH8.5.3.5 Initiate requests for contractor unescorted access to the Manager, Protective Services, for contractor employees requiring frequent and recurring access to controlled areas.

CH8.5.3.6 Ensure the appropriate personnel investigative forms for Non-Sensitive or Noncritical-Sensitive Position, and an SF 258, Fingerprint Card, are submitted to Protective Services by contractor employees requiring unescorted access to controlled access areas.

CH8.5.3.7 Immediately notify Protective Services of all employees who no longer require access.

CH8.5.4 Employees shall:

Understand and comply with procedures established to restrict access to controlled access areas.

CH8.5.5 The Review/Certification Board shall:

CH8.5.5.1 Administer cases where individuals have been denied unescorted access to a controlled access area.

CH8.5.5.2 Afford the employee the opportunity to request an administrative hearing at which the individual may confront and cross-examine witnesses, offer witnesses and other evidence in his/her behalf, and be represented by legal counsel. The hearing shall be held within reasonable proximity to the individual's work site.

CH8.5.5.3 Make recommendations to the Center Director who shall make the final decision.

Chapter 9

LOCK AND KEY PROGRAM

CH9.1 General

MSFC resources shall be protected against loss, theft, vandalism, espionage, sabotage, and other threats or acts of violence. Entry to MSFC facilities shall be controlled consistent with the mission being performed, existing vulnerabilities, and postulated threat.

CH9.2 Procedure

CH9.2.1 Master keys shall be handled under a continuous receipt system and shall not be removed from the Center. Master keys shall be issued only to Protective Services.

CH9.2.2 Keys shall be issued by Protective Services only to Lock and Key Coordinators. Lock and Key Coordinators shall, in turn, issue keys on an MSFC Form 4228, "Key Justification," to MSFC employees and associated contractor employees on an authorized-need basis.

CH9.2.3 Keys shall be issued when there is an established need based on the following criteria:

CH9.2.3.1 The building is opened and secured by the occupants.

CH9.2.3.2 Frequent and recurring access to a locked building is required during non-duty hours.

CH9.2.3.3 The room or area contains valuable or sensitive equipment and supplies which shall be protected.

CH9.2.3.4 The room is approved for open storage of Administratively Controlled Information (ACI).

CH9.2.4 Only MSFC security locks shall be used to secure gates, buildings, and rooms. Where feasible, exterior building entrances shall be secured by internal fasteners.

CH9.2.5 The number of keys issued per lock shall be limited to six, for accountability/inventory purposes. All exceptions shall be approved by the Manager, Protective Services.

CH9.2.6 Keys shall not be issued for the convenience of an individual. An unlock service is available from Protective Services Control Center.

CH9.2.7 MSFC security locks shall not be used to secure toolboxes, cabinets, and other such containers. Locks for these types of containers shall be obtained through regular supply channels.

CH9.3 Responsibilities

CH9.3.1 Protective Services shall:

CH9.3.1.1 Serve as custodian of the MSFC security lock and key system to include stocking, installing, and removing locks; making and issuing keys; managing the master key system; and maintaining all elements of the system.

CH9.3.1.2 Review all requests for locks and keys, arrange lock installations, and issue keys.

CH9.3.1.3 Approve requests for lock and key service. Requests not approved shall be returned to the originator with an explanation as to why the request was not approved.

CH9.3.1.4 Maintain records of keys issued and locks installed and annually validate records against inventories submitted by each Lock and Key Coordinator.

CH9.3.1.5 Determine initial requirements for locks on new buildings and fenced areas and ensure the required locks are installed.

CH9.3.1.6 Make periodic and random physical security surveys to ensure:

a. Redundant locks are kept to a minimum.
b. Areas requiring protection are properly secured.
c. Locks not needed are removed and returned to stock.

CH9.3.1.7 Investigate reports of lost keys and take action as appropriate.

CH9.3.2 Directors, Managers of Offices and Directorates shall:

CH9.3.2.1 After considering the sensitivity of information/material or property protection needed within an office/area, determine if the office/area should be locked after hours. If the determination is made that the area needs to be secured after hours, ensure that an MSFC Label 45 is posted outside the door. If a Label 45 is posted and the area is found to be unsecured after hours, the security officers shall complete a Report of Incident and forward copies to the Key Coordinator and the appropriate Director or Department Manager.

CH9.3.2.2 Appoint a Lock and Key Coordinator, as required, to request, account for, and control all keys issued for their areas of responsibility.

CH9.3.2.3 The Manager, Protective Services, shall be advised by memorandum of the name, telephone number, and office symbol of the appointee.

CH9.3.2.4 Internal procedures shall be developed for requesting locks and keys and ensuring that employees leaving an organization return keys.

CH9.3.3 The Lock and Key Coordinator shall:

CH9.3.3.1 Request locks and keys through the electronic Service Request System (SRS) . The location of lock installation, number of keys required, and a full justification shall be furnished.

CH9.3.3.2 Pick up and sign for all keys from Key Control, Building 4312.

CH9.3.3.3 Return the MSFC Form 4228, signed by the key holder and coordinator, to Key Control.

CH9.3.3.4 Account for all locks and keys issued to their area of responsibility, and issue keys to employees with instructions for safeguarding the keys. Return the keys when no longer needed.

CH9.3.3.5 Conduct an annual physical inventory of keys, and return keys no longer required.

CH9.3.3.6 Complete and forward through the electronic Service Request System (SRS), Lost Key Justification, within 24 hours of notification of the loss.

CH9.3.3.7 Clear employees who leave, transfer, or go on leave of absence for 90 days or longer.

CH9.3.3.8 Store available keys in locked containers when not issued or not in personal possession.

CH9.3.3.9 Upon departure, coordinate with Protective Services to ensure keys are accounted for and transferred to a succeeding Lock and Key Coordinator.

CH9.3.4 Key Holders shall:

CH9.3.4.1 Employees who are issued Government keys shall be responsible for safeguarding them at all times, and immediately report the loss of a key to the Lock and Key Coordinator. Negligence in protecting Government keys may be cause for disciplinary action.

CH9.3.4.2 Use keys for official business only and allow only authorized individuals to use their keys. Do not loan a Government key to anyone except those authorized.

CH9.3.4.3 Never take Government keys overseas unless specifically required for facility access.

CH9.3.4.4 Return all keys to the Lock and Key Coordinator upon leaving the organization.

CH9.3.5 The Locksmith shall:

CH9.3.5.1 Service and repair vaults, safes, door locks, and padlocks with three-position combination locks.

CH9.3.5.2 Cut keys and replacements, combinate and recombinate lock cores, assist in real-time response, and support Protective Services on key inventories, as necessary.

CH9.4 Lock and Unlock Services

CH9.4.1 Employees requesting access to a facility or door shall get prior approval from the key holder, key coordinator, or manager of that area. Lock/unlock services may be obtained by calling 544-HELP, #1 (544-4357).

CH9.4.2 Lock and unlock services required to support operational requirements shall be coordinated in advance with Protective Services.

CH9.5 Emergency Access

The Contract Security Service shall maintain master keys of registered locks for use during an emergency. Emergency lock and key support is available 24 hours a day by contacting 544-HELP, #1.

Chapter 10

IDENTIFICATION BADGES

CH10.1 Identification badges are required for Center Access and shall be visibly worn at all times while on Center.

CH10.2 MSFC Access Controls

CH10.2.1 MSFC is patrolled by a uniformed contract security force tasked with preventing access to MSFC property by unauthorized persons. Persons without visible identification shall be challenged, asked to produce identification, and be escorted from the Center, if appropriate.

CH10.2.2 Access to MSFC shall be controlled by issuing permanent identification badges for MSFC employees and associated contractors. In addition, temporary badges shall be issued to visitors and invited guests. Vendors, consultants, suppliers, and service representatives shall be badged through the prime contract that they are supporting. Issuance of identification badges for personnel access to MSFC property shall be managed and controlled by the Identification and Registration Section, Building 4312.

CH10.2.3 Access is a privilege which may be denied, suspended, or revoked, and shall be granted only when it furthers the conduct of NASA business.

CH10.2.4 Appropriately badged NASA employees or contractors, who are U.S. citizens, may serve as an official escort for visitors, when required.

CH10.2.5 Identification badges shall not be used as a basis for determining whether an employee has been granted a security clearance or has a need-to-know. Contact Protective Services for assistance when verifying personnel security clearance status prior to granting access to classified information.

CH10.3 Responsibilities

CH10.3.1 Protective Services shall:

CH10.3.1.1 Establish requirements for entry to MSFC, its component facilities, and its controlled access areas.

CH10.3.1.2 Ensure identification badges are controlled and issued in accordance with the instructions in this policy and applicable NASA directives.

CH10.3.1.3 Ensure all persons visiting MSFC or its component facilities wear an approved identification badge. Contractor badges issued by other NASA Centers, off-site contractor company badges, and badges from other Government agencies are not authorized for access to

MSFC property, with the exception of badges issued by Redstone Arsenal and Michoud Assembly Facility (MAF).

CH10.3.1.4 Provide training for NASA and contractor personnel authorized to sign MSFC Form 1739 Contractor Badge/Decal Application. Authorization to sign the MSFC Form 1739 is granted only after employees have been trained and have signed MSFC Form 1739-1, Signature Card.

CH10.3.2 The Identification and Registration (I&R) Section shall:

Under the direction of Protective Services, rigidly control, process, fabricate, and issue permanent and temporary identification badges for MSFC organizational elements, associated contractors, and visitors. Identification badges shall be issued at Buildings 4312, 4200, or Intergraph unless otherwise directed by Protective Services.

CH10.3.3 NASA Organizations Sponsoring Badge Applications for Contractor or Vendor Support personnel. Contracting Officer Representatives (COR), Contracting Officer Technical Representative (COTR), or technical managers who sponsor application for non-NASA (contractor or vendor) identification badges shall:

CH10.3.3.1 Complete relevant sections of the MSFC Form 1739, Contractor Badge/Decal Application and submit it in accordance with written directions and training provided by Protective Services. This dual-purpose form consolidates the request for contractor identification badges and vehicle passes.

CH10.3.3.2 Ensure foreign nationals applying for identification badges complete the appropriate background investigation paperwork, and are not issued a badge until approved by Protective Services and/or NASA Headquarters.

CH10.3.4 The Human Resources Department shall assist new NASA employees, retirees, payload specialists, and military and civil service detailees in requesting NASA identification badges and vehicle passes by completing MSFC Form 4, NASA Employee Badge/Decal Application card.

CH10.3.5 The Media Relations and Government and Community Relations Departments shall submit a request to Protective Services within 3 to 5 working days for preparation of appropriate visitor badges for VIP and/or other groups, as required.

CH10.3.6 The Procurement Office shall, through appropriate contract provisions, ensure that contractors are tasked with complying with requirements of this procedure.

CH10.3.7 Organizations Applying for Contractor/Vendor Identification Badges

Company-designated officials; e.g., Contractor Security Officer, construction superintendent, or project manager who provides assistance to non-NASA employees applying for MSFC identification badges or vehicle passes, shall:

CH10.3.7.1 Ensure company employees visiting or working at MSFC have received a security orientation and are familiar with relevant provisions of this procedure, including proper usage, safeguarding, and return of badges.

CH10.3.7.2 Complete relevant sections of the front side of the MSFC Form 1739, Contractor Badge/Decal Application, in accordance with written directions provided by Protective Services, and return to the appropriate MSFC sponsor. This dual-purpose form consolidates the request for contractor badges and vehicle passes.

CH10.3.7.3 Prime contractors shall be responsible for badges issued under their own authority and those requested by their subcontractors, vendors, suppliers, and service representatives.

CH10.3.7.4 Ensure employees who leave the company immediately return all MSFC-issued identification badges, key cards, vehicle passes, keys, etc., and clear the Center using MSFC Form 383-1, Contractor Employee Clearance Document, as a checklist. When an employee is terminated "for cause," the company representative shall confiscate all badges, key cards, keys, vehicle passes, etc., and **immediately** notify Protective Services of the termination. The company representative shall then clear the employee using MSFC Form 383-1.

CH10.3.8 Employees shall report knowledge or suspicion that requirements regarding the proper use of identification badges have been violated to Protective Services.

CH10.4 Display and Control of Badge

CH10.4.1 Each person authorized access to MSFC shall adhere to the following rules concerning the wearing and use of badges and passes:

CH10.4.1.1 The badge shall be worn above the waist, plainly visible, face side out, at all times while on MSFC or component facilities. Badges may be inserted into clear plastic holders. Safety-approved necklace material is available at Protective Services for employee use.

CH10.4.1.2 Items such as tape, pins, clips, etc., shall not be fastened to the badge in such a manner as to obstruct, alter, or in any way change the appearance of the badge. Damage to the embedded card access technology may occur if badges are altered.

CH10.4.2 Identification badges shall be safeguarded when not in use. All reasonable effort shall be made to minimize the loss or the unauthorized use of the badge.

CH10.5 Lost, Forgotten, and Replacement Badges

CH10.5.1 Badges that are faded, separated, or otherwise in poor condition shall be replaced. Badges shall be replaced when the assigned owner's physical appearance is changed; e.g., beard growth or removal, plastic surgery, or when there is a name change.

CH10.5.2 Lost or missing identification badges shall be reported to the I&R section immediately. If the employee knows the badge has been permanently destroyed or lost, a new identification badge may be issued immediately. Otherwise, a temporary badge shall be issued for up to 10 days to permit continued access to MSFC property and component facilities, and to allow the employee an opportunity to conduct a thorough search for the original picture badge. If the badge is not located after 10 days, a new identification badge may be issued by the I&R section. If a badge is lost a second time, a request for a new badge shall be submitted in writing to Protective Services explaining the circumstances of the loss.

CH10.5.3 Official visitor badges shall be issued by the I&R section to MSFC employees who report to work without a permanent badge. This badge is normally limited to one day. Valid identification is required.

CH10.6 Surrender of Badges

CH10.6.1 Employees shall comply with any reasonable request by security staff, management, or Government auditors to surrender the badge or pass for physical inspection. As a minimum, badges shall be promptly surrendered upon termination and expiration of contract.

CH10.6.2 Termination, Disciplinary or Leave of Absence

CH10.6.2.1 Employees who are on disciplinary or long-term administrative leave shall turn in their badges to Human Resources to hold until the leave is terminated.

CH10.6.2.2 Employees who go on a leave of absence for over 90 days shall turn in their badge to Protective Services. The badge shall be returned to them when they return to duty.

CH10.7 After Hours Access to MSFC

CH10.7.1 After Hours Access by Civil Service Employees

After hours access to MSFC property and component facilities by employees possessing a valid NASA identification badge is generally unrestricted, unless otherwise restricted by special safety or security requirements. Employees who are not authorized a key or keycard required to open a locked facility or work area shall make prior arrangements to enter a work area after normal duty hours.

CH10.7.2 After Hours Access by Contractor/Vendor Employees

Unescorted after-hours access by contractor/vendor employees shall be limited to those employees requiring frequent and recurring access in performance of a contract, and only at specific locations designated by the COTR on an MSFC Form 1739.

CH10.8 Types of Permanent Badges

A permanent identification badge is issued for civil service, contractors, vendors, and other assigned Government employees.

CH10.8.1 NASA Identification Badge

CH10.8.1.1 A unique NASA photo-identification badge shall be issued to all MSFC employees, military detailees, NASA Exchange employees, Intergovernmental Personnel Act (IPA) detailees, and civil service detailees. To receive a badge, MSFC Form 4, NASA Employee Badge/Decal Application, shall be completed.

CH10.8.1.2 The unique badge permits access into all general areas at MSFC, component facilities, and to other NASA Centers, unless otherwise restricted by special safety or security measures. The unique technology coded badge grants access into those areas electronically controlled by the Marshall Access Control System (MACS). The MACS system provides automated control and accountability of personnel through the use of a card reader system.

CH10.8.1.3 NASA identification badges shall normally be issued during normal hours by the I&R section.

CH10.8.2 Contractor/Vendor Badges

CH10.8.2.1 A unique MSFC identification badge shall be issued to contractors, following determination by MSFC management that frequent and recurring access to MSFC and component facilities, at least two times per week, is needed in performance of a contract. This unique badge permits normal business hours access to general areas of MSFC and component facilities, unless otherwise restricted by special safety or security measures. Only those contractors whose work site is in the vicinity of Huntsville, Alabama, and whose home address is within driving distance of MSFC shall be issued a permanent badge. NOTE: Identification badges issued to MAF employees shall be honored at MSFC.

CH10.8.2.2 To obtain a Contractor/Vendor badge, a favorable background investigation shall be conducted, and an MSFC Form 1739, “Contractor Badge/Decal Application,” shall be completed by the Contractor Security Officer or designee and submitted to the Contracting Officer Technical Representative for approval. The MSFC sponsor shall have full knowledge of contractor access requirements and limitations.

CH10.8.2.3 The MSFC representative of the sponsoring organization shall review and approve the MSFC Form 1739 and designate the NASA security zone or specific building access when after-hours access is required.

CH10.8.2.4 The contractor employee shall take the approved application to the I&R section during normal duty hours for issuance of the badge.

CH10.8.2.5 The contractor badge shall reflect the company and the contract expiration date on the front side of the badge.

CH10.8.2.6 A favorable background investigation shall be conducted for contractor foreign nationals prior to issuing a uniquely coded identification badge. Contact Protective Services for assistance. (Also see MPR 1371.1 for details on processing foreign national visits).

CH10.8.3 Retiree Card

CH10.8.3.1 A unique "retiree" identification (ID) card shall be issued to NASA retirees upon request. This distinctive ID is not valid for access to any NASA center, but shall be used to facilitate getting a visitor badge for official business.

CH10.8.3.2 To obtain a "Retiree" ID, an MSFC Form 4, "NASA Employee Badge/Decal Application," shall be completed, signed by Human Resources, and submitted to the I&R section, for issue.

CH10.8.3.3 The badge shall not be used for the purpose of soliciting or promoting activities which result in the retirees' personal gain, or for sales, services, or arranging job interviews. Noncompliance may result in revocation of privileges and recovery of the badge.

CH10.9.4 Center Activities Badge

CH10.9.4.1 Non-NASA members shall register with the Health Club, complete a personal data card, and report to the I&R section, for issue of a badge. A favorable background investigation shall be conducted.

CH10.9.4.2 Retirees who are involved in Center activities shall request a Center Activities badge, which grants them access to MSFC only, and a maximum of two vehicle decals. The Center activities badge does not grant retirees full access to MSFC facilities. Center activities that a retiree may access are:

- NASA Exchange Store, Barbershop, and cafeteria in Building 4203 during Center working hours
- Activities involving Gun, Archery, Skeet, and Trap Clubs, etc.
- Automotive Repair Shop
- Recreational ball fields, tennis courts, and picnic areas

- MSFC Wellness Center (gym), with membership
- Heritage Gallery in Lobby of Building 4200 during Center working hours

CH10.9.5 Associate Badges

A unique photo identification badge shall be issued to any US citizen that drives onto Redstone Arsenal in an established carpool with an MSFC employee; to persons who have been authorized by a child's MSFC parent to pick up and drop off children at the Marshall Child Development Center (MCDC); or to persons that participate in MARS Club or sporting activities. The badge shall be issued solely for these purposes, and shall be valid for one year or until the end of the sporting season. By signing the application for an associate badge, the sponsor accepts full responsibility for the associate and acknowledges that the badge is issued for the purpose stated. The sponsor shall ensure the badge is returned upon request by Protective Services or when no longer required for the purpose issued. The associate shall be subject to a favorable background check.

CH10.10 Badging for Non-U.S. Citizens

Non-U.S. citizens shall be badged only after approval of the International Visit Coordinator. See MPR 1371.1.

Chapter 11

VEHICLE REGISTRATION

CH11.1 All vehicles accessing the Center shall be registered.

CH11.2 Responsibilities

CH11.2.1 Protective Services shall:

Ensure vehicle passes are controlled and issued in accordance with the instructions in this policy.

CH11.2.2 The Protective Services shall:

Issue a maximum of four permanent vehicle decals (motorcycles and bicycles included) to qualified Government employees or associated contractors. Retirees who have been issued an ID for Center activities may be issued a maximum of two decals. Under the direction of Protective Services, rigidly control and issue permanent and temporary vehicle passes to persons authorized to operate motor vehicles on facilities under MSFC jurisdiction.

CH11.2.3 Employees, Retirees, and Contractors/Vendors shall:

CH11.2.3.1 Have a valid state driver's license in their possession at all times while driving on Government property.

CH11.2.3.2 Ensure registered motor vehicles meet the safety standards prescribed by the statutes of the state in which the vehicle is registered.

CH11.2.3.3 Maintain proof of public liability insurance coverage for their motor vehicle.

CH11.2.3.4 Immediately report the removal of a decal from their vehicle to Protective Services.

CH11.2.3.5 Register motorcycles and provide proof that they have completed the required safety class for operation of a motorcycle.

CH11.3 Applying for Permanent Vehicle Decals

CH11.3.1 MSFC employees, retirees, and contractors shall provide relevant vehicle information and certification of liability insurance to the I&R Section. Assigned active-duty or retired military personnel may elect to obtain their decals through the Provost Marshal's Office, Redstone Arsenal.

CH11.3.2 Applicant for decal shall present a valid state driver's license, proof of insurance, proof of ownership (e.g., bill of sale, license registration, or vehicle title), and a NASA identification badge.

CH11.3.2.1 If the vehicle is not owned or leased by the registrant, written justification shall be provided to describe why the vehicle shall be used onsite and for how long.

CH11.3.2.2 A letter of permission from the vehicle owner authorizing registration shall be required, along with proof of ownership, and certification that the owner has the appropriate liability insurance.

CH11.3.3 Permanently affix the decal on the outside of the lower left corner of the windshield, driver's side of the vehicle. Decals shall not be used on other than the vehicle for which it was issued. Temporary vehicle passes shall be displayed on the inside of the left corner, driver's side, of the vehicle.

CH11.3.4 Decal remains shall be returned to the I&R Section when the vehicle is sold or disposed of, prior to termination, upon expiration of contract, upon suspension of driving privileges, or when recalled by Protective Services. When the decal cannot be returned; e.g., because of vehicle theft, the registrant shall notify Protective Services immediately.

CH11.3.5 Widows and widowers of retirees shall be issued one decal if they use the MARS club.

CH11.4 Applying for a Temporary Vehicle Pass

CH11.4.1 Visitors who operate motor vehicles on MSFC shall go to Protective Services to obtain a Temporary Vehicle Pass. A Temporary Vehicle Pass shall not normally be issued for longer than 30 days. Appropriately badged individuals are not required to register vehicles for a one-day visit because they are issued a one-day pass at the gate.

CH11.4.2 A temporary Vehicle Pass may be obtained in lieu of a permanent decal whenever possession of a borrowed, leased, or rented vehicle is not expected to exceed 30 days.

CH11.4.3 When the vehicle pass is no longer required, but time has not expired, the visitor shall return the pass to Protective Services.

Chapter 12

TRAFFIC ENFORCEMENT AND PARKING

CH12.1 General

MSFC has adopted the Redstone Arsenal Traffic Regulations, AMCOM Regulation 210-2 (copy in Protective Services), and shall enforce these regulations on MSFC property. All vehicle and pedestrian traffic is governed by the provisions of the Alabama State Vehicular and Pedestrian Traffic Laws, as well as the instructions contained in this.

CH12.2 Responsibilities

CH12.2.1 The Center Director shall:

Prescribes traffic regulations applicable to MSFC property. MSFC shall enforce traffic regulations on MSFC property, while the Provost Marshal shall enforce those regulations applicable to Redstone Arsenal, exclusive of MSFC property.

CH12.2.2 The Manager, Protective Services, shall:

CH12.2.2.1 Enforce all MSFC traffic regulations on MSFC property.

CH12.2.2.2 Report traffic violations of MSFC employees to the individual through the employee's supervisor.

CH12.2.2.3 Report traffic violations by other individuals to the employer or home address.

CH12.2.2.4 Investigate all traffic violations and accidents occurring on MSFC property.

CH12.2.2.5 Bring certain violations to the attention of the Army Provost Marshal's Office for issuance of a U.S. Magistrate's Court citation, if warranted. The Manager, Protective Services, shall follow the guidance of the Chief Counsel's Office on matters involving court citations.

CH12.2.2.6 Immediately impound unattended vehicles which constitute a safety hazard when the owner or driver cannot be located. All other vehicles considered unattended shall be cited and the owner shall have 3 days from the date of the citation to remove the vehicle before impoundment action is initiated. An owner or driver who refuses to move his/her vehicle shall be charged for the cost of removal.

CH12.2.2.7 Enforce all parking regulations.

CH12.2.2.8 Maintain the records of all traffic violations on MSFC property.

CH12.2.2.9 Assess points for violations according to the Point Assessment Table. All assessment notices shall include the total number of points accumulated within the reckoning period.

CH12.2.2.10 Initiate action to suspend driving privileges for drivers who have been assessed 12 traffic points in a 24-month reckoning period.

CH12.2.2.11 Issue Service Vehicle Parking Permits.

CH12.2.3 Facilities Engineering Department shall:

CH12.2.3.1 Obtain, install, or maintain painted curbs, parking bumper-rails, and traffic control signs that are required for traffic control when approved by Protective Services.

CH12.2.3.2 Paint or remove handicapped spaces when approved by the Equal Opportunity Office.

CH12.2.4 Vehicle Operators on MSFC and Redstone Arsenal (RSA) shall:

CH12.2.4.1 Obey all traffic regulations on MSFC and RSA.

CH12.2.4.2 Possess a motor vehicle driver's license recognized by the State of Alabama as a valid driver's license.

CH12.2.4.3 Comply with all state statutes concerning licensing of drivers and Alabama Financial Responsibility Laws at all times. Any driver or owner who fails to comply may have his/her driving privileges suspended by the Manager, Protective Services. This suspension shall remain in effect until the individual produces, in person, proof of insurance or proof that they have assumed the necessary financial responsibilities. Vehicles registered at component facilities shall meet the statutes of that state.

CH12.2.4.4 Park only in authorized parking spaces and observe all parking restrictions in areas where official signs, other markings, or operations prohibit or restrict parking.

CH12.2.4.5 Parking of privately owned or government vehicles in fire lanes, or within 15 feet of a fire hydrant or an outside Fire Department sprinkler connection, is prohibited except for loading or unloading of personnel or equipment.

CH12.2.4.6 Vehicles shall go no faster than 15 miles per hour in parking areas and 25 miles per hour on roadways where speed limits are not posted.

CH12.2.4.7 When advised by siren or other emergency warning device of the approach of an emergency vehicle, pull to the right hand curb and stop, being clear of any intersection, and

remain there until the emergency vehicle has passed, unless otherwise directed by MSFC Protective Services.

CH12.2.4.8 In the event of a traffic accident employee shall:

a. Summon a security officer, or a military police officer if the accident occurs on Army-controlled property.

b. Give name, address, rank (if military), serial or badge number, organization, and show driver's license (when requested) to the investigating officer.

c. Remain at the scene of the accident unless they must leave to summon aid.

d. If driving a Government-owned or Government-contracted vehicle, complete Standard Form 91, Operator's Report of Motor Vehicle Accident.

CH12.2.4.9 If involved in a traffic accident resulting in injury or death employee shall:

a. Call for an ambulance.

b. Render reasonable assistance to the injured.

c. Remain at the accident scene until medical assistance arrives.

d. Assist medical personnel, as directed, until the injured person or persons are under the complete supervision of the medical personnel.

CH12.3 Point Assessments

Any person who is charged with a violation of MSFC or Alabama/Traffic Regulations shall be assessed points against his/her driving record according to the following point assessments:

OFFENSE	POINTS ASSESSED
Driving under the influence	12
Leaving the scene of an accident involving Death or personal injury	12
Operating a vehicle with suspended permit or Driving privileges	12
Leaving the scene of an accident without showing ID	6
Owner knowingly permits operation of vehicle by Person under influence	6
Making a false statement that a decal has been destroyed	6
Reckless driving	6
Improper passing	4
Failure to obey officer's signal	4
Failure to obey traffic signal or stop sign	4
Following too closely	4
Failure to yield	4
Driving without a license	4
Failure to comply with MSFC vehicle registration requirements	4
All other moving violations	3
Cell phone use while driving	2
Failure to report an accident when required by regulation or law	2
Operating an unsafe vehicle	2
No proof of insurance	2
Seat belt violation	2
Child restraint violation	2
Improper/expired tag	2
Use of radar or laser-detecting devices to indicate the presence of speed recording instruments or to transmit simulated erroneous speeds	2
Speeding: 10 MPH over 11-15 MPH over 16-20 MPH over 20 or more MPH over	 3 4 5 6

OFFENSE	POINTS ASSESSED
PARKING AND OTHER VIOLATIONS:	
Fire Hydrant/Fire Lane/Safety Hazard	4
Handicap space	3
Parking on grass or seeded area	2
Improper Parking (not parking within a marked or designated parking space)	2
Reserved space	2
Government/Service Vehicle space	2
Decaled vehicle parked in visitor space	2
Transient at assigned area	2
Transient over time limit	2
Disregard of posted notices	2
No parking area	2

When two or more violations are committed on a single occasion, the points assessed shall be for the offense having the greater value.

CH12.4 Appeals and Administrative Review – NASA Civil Service Employee

CH12.4.1 Traffic citations

If a driver believes that the issuance of a traffic citation and assessment of points were unwarranted, or that there were extenuating circumstances, he/she may initiate an appeal.

CH12.4.2 Grievances

NASA employees may initiate a grievance in accordance with the following instructions:

CH12.4.2.1 Association of Federal Government Employees (AFGE) bargaining unit members shall file grievances with the involved supervisor, Manager, Protective Services.

CH12.4.2.2 Marshall Engineers and Scientists Association (MESA) and non-bargaining unit members shall file grievances with their immediate supervisor who, in turn, shall forward the grievance to the Manager, Protective Services.

CH12.4.2.3 If the decision by the Manager, Protective Services, is unacceptable to the grievant, the grievance shall progress through an appeals process. For AFGE and MESA members, the appeals process shall be in accordance with the union agreements. For non-bargaining unit members, the process in paragraph CH12.5.1.2 below shall be followed.

CH12.4.3 Suspension of Driving Privileges – NASA Employees

CH12.4.3.1 When a driver accumulates 12 or more traffic points in a 24-month period, the Manager, Protective Services, shall notify the driver through his/her organization in writing that driving privileges shall be suspended for 180 days from the date of notification. If the suspended employee is caught driving during this period, an additional two years shall be added to the suspension. If caught a second time, the matter shall be referred to Human Resources for proper personnel action.

CH12.4.3.2 The suspension notification shall be forwarded to the driver within 10 workdays of the final appeal expiration date of the last traffic citation issued, instructing the driver as to what action he/she shall take.

CH12.4.3.3 Suspension of driving privileges is normally not invoked until all time limitations for appeal have expired. However, suspension of driving privileges shall be invoked at any time if it is thought the driving privileges endanger the health or safety of other employees.

CH12.4.3.4 Suspension of driving privileges shall also result in action to revoke an employee's right to operate a Government vehicle in the performance of official duties.

CH12.4.3.5 A driver may appeal the suspension of driving privileges through the appropriate grievance procedure.

CH12.5 Appeals and Administrative Review – Non-Civil Service NASA Employees

CH12.5.1 Traffic Citations

If a **non**-Civil Service NASA employee (e.g., contractor employee) believes that the issuance of a traffic citation and the assessment of points were unwarranted, or that there were extenuating circumstances, he/she may initiate the following:

CH12.5.1.1 Submit a written request to the Manager, Protective Services, for an administrative review describing the reasons for the request and the remedy requested. The appeal shall be delivered to the Manager, Protective Services, no later than 30 workdays from the date of notification of assessment.

CH12.5.1.2 If the request for an administrative review is denied, the driver may appeal to the Director, Center Operations, within 10 workdays from the date of denial by the Manager, Protective Services. The decision of the Director, Center Operations, shall be final.

CH12.5.2 Suspension of Driving Privileges – Non-Civil Service NASA Employees

CH12.5.2.1 When a driver accumulates 12 or more traffic points in a 24-month period, the Manager, Protective Services, shall notify the driver in writing that his/her driving privileges shall be suspended 10 workdays from the date of the notification.

CH12.5.2.2 The notification shall be forwarded to the driver within 10 workdays of the final appeal expiration date of the last traffic citation issued. It shall contain instructions for the action the driver is to take, and shall advise the driver that an administrative review by the Manager, Protective Services, may be requested.

CH12.5.2.3 The driver may, within 30 workdays from the date of the suspension notification, request, in writing, an administrative review by the Manager, Protective Services. Within 10 workdays, the Manager, Protective Services, shall provide the appellant with a written response.

CH12.5.2.4 If the driver is not satisfied with the decision, he/she may appeal the suspension to the Director, Center Operations, within 10 workdays after the date of the decision.

CH12.5.2.5 The appeal shall be in writing. The appellant has the right to personally present evidence and arguments to the Director, Center Operations. If a personal hearing is desired, it shall be requested in the written appeal.

CH12.5.2.6 The Director, Center Operations, shall render a written decision as soon as possible after receipt of the appeal. The decision shall be to sustain, reduce, modify, or revoke the suspension. This decision shall be final.

CH12.5.2.7 Suspension of driving privileges is not normally invoked until all the time limitations for appeal have expired. However, suspension of driving privileges shall be invoked at any time if continued driving privileges endanger the health or safety of other employees.

CH12.5.2.8 Suspension of driving privileges shall also result in action to revoke an employee's right to operate a Government vehicle in the performance of official duties.

CH12.6 Referral of Serious Offenses to the U.S. Magistrate

In addition to the assessment of points, the Manager, Protective Services, may, with the concurrence of the Chief Counsel, refer offenses to the U.S. Magistrate's Office.

CH12.7 Issuing Service Vehicle Permits

Service Vehicle Permits may be issued by Protective Services to companies for use in unmarked vehicles used by their service personnel. Requests shall be submitted in writing to Protective Services by the manager or security officer and shall be fully justified. Requests for Service Vehicle Permits for privately owned vehicles shall be accompanied by the required documentation substantiating the proof of mileage reimbursement for on-Center use.

Chapter 13

Control of Firearms and Prohibited Items

CH13.1 General

CH13.1.1 Privately owned firearms, weapons, and explosives shall be controlled as outlined in U.S Army Aviation Missile Command (AMCOM) regulations (AMCOM Regulation 210-2, Appendix Y).

CH13.1.2 The introduction or possession of firearms and other prohibited items at MSFC without written authorization is prohibited, except under strict conditions approved by the Manager, Protective Services. Possession includes not only having items on one's persons, but also having items under personal control, i.e., in vehicles or offices.

CH13.1.3 This procedure excludes those authorized under the National Aeronautics and Space Act of 1958; Law enforcement officers from city, county, state, or federal departments or agencies; MSFC contract security force in the performance of official duties; and recreational groups specifically authorized by the Manager, Protective Services.

CH13.2 Conditions Under Which Firearms May be Carried

CH13.2.1 Federal and local law enforcement personnel may possess weapons on MSFC property when performing official duties.

CH13.2.2 Firearms may be permitted on a case-by-case basis in connection with specific activities sponsored by approved MSFC recreational organizations. Appropriate state and local permits for carrying a weapon shall be met.

CH13.2.3 Firearms shall not be carried in such a manner as to preclude knowledge of its presence by direct observation, except by sworn law enforcement officers and others specifically authorized by the Manager, Protective Services. Loaded firearms shall never be transported on MSFC by personnel other than law enforcement officers and others specifically designated by the Manager, Protective Services.

CH13.2.4 Members of the Marshall Activities and Recreation Society (MARS) Skeet Club, or other approved sponsor of on-site activities involving the use of firearms, are authorized to possess firearms under specific conditions. The MARS Skeet Club shall be responsible for instructing members in the safe use and transportation of firearms in accordance with the National Rifle Association (NRA) standards and this regulation.

CH13.3 Reporting Requirements

MSFC employees who become aware of the presence of unauthorized or suspected prohibited weapons on MSFC shall immediately notify the Protective Service Control Center at 544-HELP, #1. If the status of a weapon or item is questionable, Protective Services shall be notified for investigation, as appropriate.

CH13.4 The following items shall be prohibited:

CH13.4.1 Personal firearms and ammunition, unless authorized by Protective Services.

CH13.4.2 Air rifles or pistols, crossbows, or any bow drawn, held, or released by a mechanical device.

CH13.4.3 Switch-blade or spring opening knives regardless of length (pocket knives may be carried concealed on ones person if the blade folds in and is no longer than 3 inches in length). Razors, ice picks or any like item carried concealed on a person are also prohibited.

CH13.4.4 Throwing knives.

CH13.4.5 Blackjacks, saps, slaps, clubs, or any other like device designed or intended to be used to strike a blow.

CH13.4.6 Metal knucks, knuckles, throwing stars, num-chucks, or any other like hand-fitting devices designed or intended to be used to strike a blow.

CH13.4.7 Martial arts offensive or defensive weapons, except those authorized for use in recognized MARS Club activities.

CH13.4.8 Incendiary or pyrotechnic devices.

CH13.4.9 Explosives, including fireworks.

CH13.4.10 Any device or item known to, or intended to, inflict injury or death or cause property damage, or any device or item specifically prohibited by applicable city, county, state, or federal law, statute, or regulation, etc.

CH13.5 Penalties for Violating Firearms Guidelines

Persons who violate the provisions of this procedure shall be subject to administrative and criminal sanctions.

Chapter 14

COMMUNICATIONS SECURITY (COMSEC)

CH14.1 General

Communications systems and networks shall be secured by such means as are necessary to prevent compromise, denial of service, or exploitation. The NASA COMSEC Manager shall manage the overall NASA-wide COMSEC program by providing oversight and support to NASA Centers in their implementation of Center COMSEC efforts. The NASA COMSEC Manager responsibility has been delegated to the Director, NASA Security Management, or designee.

CH14.2 Responsibilities

CH14.2.1 MSFC COMSEC Account Manager shall:

CH14.2.1.1 Ensure compliance with NASA COMSEC policy at MSFC.

CH14.2.1.2 Consult with the NASA COMSEC Manager on COMSEC issues impacting MSFC, and attend COMSEC working groups or technical seminars prescribed by the NASA COMSEC Manager or Manager, Protective Services.

CH14.2.1.3 Be knowledgeable of national TEMPEST threat and vulnerability assessment methodology, and be responsible for coordinating with the NASA COMSEC Manager concerning TEMPEST countermeasure applications.

CH14.2.1.4 Conduct scheduled and unscheduled inspections of secure communications systems, facilities, and areas where classified information is processed.

CH14.2.2 Managers of MSFC Operating Organizations shall:

CH14.2.2.1 Coordinate requirements for COMSEC material and equipment well in advance of the needed date to allow sufficient time for site assessment, planning design standards, procurement of hardware, and installation.

CH14.2.2.2 Appoint an appropriately cleared and briefed Operational COMSEC Officer in writing to ensure compliance with COMSEC and cryptographic policies and procedures.

CH14.2.2.3 Ensure employee compliance with all security requirements, standards, and procedures applicable to secure MSFC communications systems.

CH14.2.3 Employees briefed on COMSEC matters shall:

CH14.2.3.1 Comply with all security requirements, standards, and procedures applicable to secure communications systems.

CH14.2.3.2 Attend required COMSEC training to become more aware of the special sensitivity and handling of COMSEC material.

CH14.3 Release of Unclassified COMSEC Material

Requests to release unclassified COMSEC material to the public domain shall be submitted to the MSFC COMSEC Manager for review/concurrence and submittal to the National Security Agency for approval.

CH14.4 COMSEC Surveys

CH14.4.1 Initial Survey

CH14.4.1.1 Protective Services shall conduct an initial survey of a proposed COMSEC project, program, or facility to assess COMSEC operating procedures, handling and storing of COMSEC material, routine and emergency destruction capabilities, and intended compliance with installation, line separation (red/black) criteria, or handling of cryptographic keys and equipment. A final survey report of the findings and recommendations shall be forwarded to the affected operating organization for review and corrective action, as necessary.

CH14.4.1.2 When a determination has been made that the proposed COMSEC facility or program conforms to all security requirements, facility or system accreditation shall be afforded and approval to commence COMSEC operations granted.

CH14.4.2 Periodic Survey

CH14.4.2.1 Random COMSEC surveys may be conducted by Protective Services to ensure COMSEC requirements are being met. As a minimum, an annual COMSEC survey shall be conducted.

CH14.4.2.2 A COMSEC survey shall be conducted by Protective Services when there is evidence of insecurity, penetration, or tampering; or, if alterations significantly change the physical characteristics of the accredited facility; or, when the facility is relocated or is reoccupied after being temporarily abandoned. A final report of findings and recommendations shall be forwarded to the affected operating organization for review and corrective action, as necessary.

Chapter 15

NASA MISSION ESSENTIAL INFRASTRUCTURE PROTECTION PROGRAM (MEIPP)

CH15.1 General

CH15.1.1 The MEIPP seeks to prevent loss, theft, vandalism, espionage, sabotage and other threats or acts of violence against NASA assets. An effective MEI protection program provides reasonable, affordable, practical, and responsible protection, within acceptable risks, to those vital NASA resources, that cannot reasonably be replaced, or have unique capabilities to support NASA goals.

CH15.1.2 The MEIPP shall apply to all MSFC operations regardless of geographic location or contractor operations.

CH15.1.3 Critical MSFC MEI resources may include vital elements of a space transportation system, associated one-of-a-kind manufacturing of test equipment, critical support facilities, or hardware/software developed or managed by MSFC. NASA MEI may also include, IT resources managed under the "Special Management Attention (SMA)" designator; critical components; communication, command, and control capability; government-owned flight or experimental flight vehicles and apparatus; and one-of-a-kind irreplaceable facilities and supporting infrastructure.

CH15.2 MSFC MEIPP Implementation Requirements

The MSFC MEIPP Implementation follows NASA Headquarters criteria and procedures in identifying and nominating NASA Assets for the NASA Mission Essential Infrastructure Protection Program (MEIPP**).**

CH15.2.1 Designated MEI assets shall be provided a level of protection commensurate with their level of criticality to the NASA mission as determined by an appropriate vulnerability risk assessment.

CH15.2.2 Minimum security requirements for MEI facilities or facilities housing MEI assets shall be:

CH15.2.2.1 A Facility Security Manager (FSM) shall be designated for each facility. The FSM shall ensure that security training is provided to employees with access to the MEI asset and that program management implements and enforces the security requirements developed for the asset.

CH15.2.2.2 An entry control system shall be employed at all times.

CH15.2.2.3 Intrusion Detection Systems (ISD) and other surveillance systems (e.g. CCTV), when required, shall be appropriately monitored and shall receive appropriate response by armed mobile security personnel capable of responding within locally established time limits but shall not exceed 5 minutes.

CH15.2.2.4 Security fencing shall be installed when the need is identified during the conduct of security vulnerability risk assessments.

CH15.2.2.5 Security lighting shall be installed at key areas around the facility to facilitate, to the extent possible, detection of intruders.

CH15.2.2.6 All personnel requiring unescorted access to the MEI shall have had the proper personnel security background investigation.

CH15.2.2.7 Personnel shall properly display issued photo ID.

CH15.2.2.8 MEI shall be designated and properly posted as a NASA "Restricted" area, at a minimum.

CH15.2.2.9 After completion of initial security vulnerability risk assessment upon designation as an MEI, reassessments shall be conducted every 2 years at a minimum, or more frequently as circumstances warrant.

CH15.3 Responsibilities

CH15.3.1 Center Director or Designee shall:

Serve as the Center Risk Acceptance Authority (RAA) and ensure vulnerability assessments of MSFC resources are conducted, MEI proposals are prepared, approved enhancements are funded, and implementing activities are carried out at MSFC, its component facilities and contractor facilities.

CH15.3.2 Managers of Program/Projects shall:

CH15.3.2.1 Review and identify all critical programs or assets managed by MSFC which warrant designation as a MEI resource and appropriate protection measures, ensuring that program planning includes proper security provisions and funding.

CH15.3.2.2 Notify, in writing, the Manager, Protective Services, and any appropriate authorities at MSFC associated contractor facilities, of critical items requiring designation as MEI and its special security measures.

CH15.3.2.3 Ensure that MSFC industry partners establish plans with detailed procedures for special security measures for critical assets. Notify the Procurement Office of all contracts that

involve the procurement of critical items to assure contractor compliance with the intent of this procedure.

CH15.3.2.4 Develop a written plan to delineate the special security measures, not covered in existing management instructions, required to protect critical hardware/software. Coordinate, as required, with the Manager, Protective Services, on matters involving protection of designated MEI resources.

CH15.3.2.5 Continually emphasize within their respective organizations the necessity for observing all security measures implemented to protect MSFC MEI assets.

CH15.3.2.6 Evaluate the results of MEI surveys of MSFC and associated contractor facilities and take appropriate action to correct deficiencies.

CH15.3.2.7 Ensure employees know the criticality of MEI facilities in which they are assigned and the security precautions employed to protect the facility.

CH15.3.2.8 Ensure that employees receive special security training from security personnel before accessing facilities or assets controlled by the MEIPP.

CH15.3.3 Director, Center Operations shall:

Upon receipt of notification that a contract is subject to the provisions of MEIPP, take the necessary actions to introduce contractually the security measures as established by the organization, based upon an MEI survey.

CH15.3.4 Manager, Protective Services shall:

CH15.3.4.1 Provide functional oversight of all MEI-related security activities carried out within MSFC.

CH15.3.4.2 Conduct annual Risk Assessments at MSFC, its component facilities and associated contractor facilities to identify and measure risks as well as develop, select, and manage options for resolving these risks. Report the survey results to the appropriate manager.

CH15.3.4.3 Ensure that all MEI assets are identified.

CH15.3.4.4 Recommend cost-effective security solutions or waivers to the RAA for specific vulnerabilities of MEI assets.

CH15.3.4.5 Advise and assist the managers of programs/projects and contractor facilities in the development of specific security requirements.

CH15.3.4.6 Report threats and unusual incidents to the Center Director and to NASA Headquarters, as appropriate.

CH15.3.4.7 Provide special security training or briefings to employees, as appropriate, related to the MEI protection program.

CH15.3.4.8 Serve as the Center Critical Infrastructure Assurance Officer(CIAO).

Chapter 16

PROGRAM SECURITY

CH16.1 General

The objective of program security is to adopt a life-cycle systems security engineering approach for NASA acquisitions by enhancing the protection of the most critical program information, technologies, or systems during the design, acquisition, and operational phase. This approach validates the threats to a system and identifies its vulnerability to compromise, prior to considering and selecting the most appropriate safeguards to reduce the risk. The security disciplines to be incorporated into the system development process shall be adequately planned and tailored to a particular program/project to build total security into the system.

CH16.2 Applicability

CH16.2.1 NASA System Acquisition Protection Management tasks shall be tailored and selectively applied to NASA contract specifications, requests for proposals, statements of work, and MSFC in-house efforts requiring protection of critical information or technologies.

CH16.2.2 The program is designed to facilitate the identification of protection requirements which are based on identified risks. Appropriate safeguards shall be engineered into the program from the beginning of the life cycle. Therefore, it accommodates research and development, test and evaluation, and system operation and modifications. Protective Services shall work closely with the program manager, prime contractors, and national intelligence agencies to continually evaluate the program sensitivity.

CH16.3 Responsibilities

CH16.3.1 Program/Project Managers shall:

CH16.3.1.1 Direct the development of a system protection plan for major system acquisitions or sensitive research and development efforts to address the issue of protecting critical information and resources.

CH16.3.1.2 Establish a process to track funding requirements for protection measures for the life-cycle of the program/project.

CH16.3.1.3 Serve as the designated approval authority.

CH16.3.2 Protective Services shall:

CH16.3.2.1 Provide functional oversight of system acquisition protection management activities carried out at MSFC.

CH16.3.2.2 Advise and assist the managers of programs/projects and contractor facilities in the development of acquisition system protection requirements.

CH16.3.2.3 Provide input into the systems engineering process and the functions related to systems development to achieve comprehensive security in developing programs/projects.

CH16.3.2.4 Develop and execute a strategy that identifies and prioritizes threats to the program/project and make recommendations for protective requirements.

CH16.3.2.5 Develop and provide a system acquisition protection management training program, as necessary, for program managers and other acquisition personnel.

CH16.3.3 The Contracting Office shall:

Upon receipt of notification that a contract is subject to the provisions of the System Acquisition Protection Management Program, take the necessary actions to introduce contractually the tailored security measures as established by the program/project manager.

CH16.4 Task Requirements

CH16.4.1 A tailored MSFC System Acquisition Protection Management Program shall be developed for each major system, consistent with other design and operational considerations, in support of the overall program objectives.

CH16.4.2 To ensure efficiency, the program shall accomplish the following:

CH16.4.2.1 Enhance the operational readiness and program success of the resource.

CH16.4.2.2 Identify and reduce potential vulnerabilities to validated threats.

CH16.4.2.3 Provide management with information essential to system security planning.

CH16.4.2.4 Minimize the impact on the overall program cost, schedule, and performance.

CH16.4.2.5 The primary output of the program begins with the identification of a broad range of security criteria and concepts which satisfy operational conditions and program requirements.

CH16.4.2.6 The various system security engineering tasks shall be evaluated for implementation during the appropriate acquisition phase.

CH16.5 Spacecraft Requirements

CH16.5.1 All spacecraft shall employ encryption protection on telemetry and cross-communication systems, this includes Flight Termination Systems (FTS). On manned systems, NSA approved Type 1 encryption shall be used.

CH16.5.2 Spacecraft navigation systems shall be based on the Precise Positioning Service of the Global Position System in addition to any other required navigation systems.

CH16.5.3 Any deviations to this policy shall be approved by the Program Manager and the Manager, Protective Services in writing.

CHAPTER 17

COUNTERINTELLIGENCE

CH17.1 Reference

NPD 1660.1, "NASA Counterintelligence (CI) Policy"

CH17.2 Applicability

NASA CI Policy is applicable to all NASA programs, projects, operations, personnel, and other activities conducted by or for NASA at NASA Headquarters and NASA Centers, including Component Facilities, and to any contractor personnel or other person or entity to the extent provided in the contract or other governing instrument.

CH17.3 General

CH17.3.1 The CI objective is to detect, deter, and neutralize the potential threat posed by foreign intelligence services, other foreign entities, and acts of terrorism.

CH17.3.2 All CI activities shall be conducted fairly, objectively, and with full regard for applicable laws and policies.

CH17.4 Responsibilities

CH17.4.1 Center Director shall:

CH17.4.1.1 Create and maintain a dedicated CI Office responsible for administering the NASA CI Program at the Center under the direction of the Manager, Protective Services.

CH17.4.1.2 Assure that the Center fully cooperates in the conduct of inquiries, investigations, and other CI activities, to the extent permitted by law.

CH17.4.1.3 Assure that Center personnel attend mandatory CI awareness and threat briefings.

CH17.4.2 Manager, Protective Services shall:

CH17.4.2.1 Provide administrative support, general guidance, and local oversight for the Center CI program.

CH17.4.2.2 Assure that the Center CI program fully integrates with other Protective Services security disciplines, i.e. Physical Security, Personnel Security, Program Security, Document Security, Technical Security, and Information Technology

Security.

CH17.4.3 Center Counterintelligence Office (CCO) shall:

CH17.4.3.1 Conduct CI inquiries and investigations.

a. Administrative inquiries shall be conducted concerning misconduct or incidents that impact the proper protection of personnel, facilities, operations, or administratively controlled, export controlled and proprietary information in a CI or counterterrorism (CT) context.

b. Preliminary inquiries shall be conducted based upon indicators of foreign intelligence methodology or indications of espionage or terrorism directed at personnel, facilities, operations, or classified, administratively controlled, export controlled, or proprietary information.

c. CI investigations shall be conducted concerning incidents or allegations of compromise or suspected compromise of classified, administratively controlled, export controlled, or proprietary information; the protection of personnel, facilities, and operations from the threats posed by espionage conducted for or on behalf of foreign or domestic powers, organizations, or persons; and domestic or international terrorist activities.

d. Joint investigations shall be conducted with other Federal agencies as appropriate.

CH17.4.3.2 Conduct CI liaison with appropriate Federal, state, and/or local agencies, contractors, and Center personnel for relevant threat information.

CH17.4.3.3 Conduct CI analysis and undertake appropriate steps to protect Center personnel, operations, and facilities from CI and/or CT threats.

CH17.4.3.4 Conduct CI/CT education and awareness training for Center personnel.

CH17.4.4 Employees shall:

CH17.4.4.1 Report all incidents of deliberate or suspected compromise of classified national security information.

CH17.4.4.2 Report all incidents of unclassified but sensitive information compromise by or on behalf of foreign or domestic powers, organizations, or persons.

CH17.4.4.3 Report all information pertaining to international or domestic terrorist activities.

CH17.4.4.4 Report such incidents and information personally, promptly, and directly to the Center CI Office. To ensure free and unimpeded reporting, an employee may ask for

confidentiality.

CH17.5 Access to records, documents, personnel, and premises in support of CI activities.

CH17.5.1 All NASA personnel and organizations, other Federal personnel or military detailees, and contractors located at the Center shall cooperate fully with the Center CI Office, to the extent permitted by law.

CH17.5.2 Such cooperation shall include:

CH17.5.2.1 Complete and free access to NASA premises, employees, files, and documents.

CH17.5.2.2 Technical consultation, examination, and assistance regarding information or evidence being developed.

CH17.5.2.3 Statements, both oral and written, including statements under oath or affirmation, with due regard to Privacy Act considerations.

CH17.5.2.4 Other such assistance as shall be required in order to complete the inquiry or investigation.